

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1346919-0

Total Deleted Page(s) = 27

Page 3 ~ b7E;  
Page 4 ~ b7E;  
Page 5 ~ b7E;  
Page 6 ~ b7E;  
Page 7 ~ b7E;  
Page 8 ~ b7E;  
Page 9 ~ b7E;  
Page 10 ~ b7E;  
Page 11 ~ b7E;  
Page 12 ~ b7E;  
Page 13 ~ b1; b7E;  
Page 14 ~ b7E;  
Page 15 ~ b7E;  
Page 16 ~ b7E;  
Page 17 ~ b7E;  
Page 18 ~ b7E;  
Page 19 ~ b7E;  
Page 20 ~ b7E;  
Page 21 ~ b7E;  
Page 22 ~ b7E;  
Page 23 ~ b7E;  
Page 24 ~ b7E;  
Page 25 ~ b7E;  
Page 33 ~ Duplicate - TO 139C-LA-127588-1A SEC 5 SERIAL 110;  
Page 50 ~ Duplicate - TO 139C-LA-127588-A SEC 6 SERIAL 342;  
Page 51 ~ Duplicate - TO 139C-LA-127588-A SEC 6 SERIAL 342;  
Page 52 ~ Duplicate - TO 139C-LA-127588-A SEC 6 SERIAL 342;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 04-27-2011 BY 60324 uc baw sab/ml

IN

DATE:07-09-94\*TIME:18:26\*

MATCHED ON:\*L/N\*F/N\* MI\*B/5

DMV RECORD FOR LAW ENFORCEMENT USE ONLY

DL/NO:C5943904\*B/D:11-27-59\*NAME:HEINZ ERIC EDWIN JR\*

RES/ADDR: AS OF 01-10-92:3640 S SEPULVEDA 107 W LOS ANGELES 90034\*

OTH/ADDR AS OF 04-22-87:10733 RIVERSIDE DR N HOLLYWOOD \*

AKA:PETERSEN JUSTIN TANNER\*

IDENTIFYING INFORMATION:

SEX:MALE\*HAIR:BROWN\*EYES:BRN\*HT:6-00\*WT:145\*

ID CARD MLD:01-29-88\*EXP/BD:93\*BATES:267\*

LIC/ISS:10-08-85\*EXP/BD:88\*CLASS:3

& M1 MOTORCYCLE\*

LATEST APP:

DL TYPE:ID CARD\*ISS/DATE: 12-30-87\*OFFICE: GLN\*

RESTR:CLASS C/3 DRIVING LIMITED TO VEHICLE WITH AUTOMATIC TRANSMISSION,

LICENSE STATUS:

EXPIRED\*

DEPARTMENTAL ACTIONS:

NONE

CONVICTIONS:

NONE

FAILURES TO APPEAR:

NONE

ACCIDENTS:

NONE

END

OUTPUT MSG 902,

FROM CL10 FOR FBI4

07/09/94 18:26

65X-LA-126522-63

SEARCHED _____	INDEXED _____
SERIALIZED <u>h</u>	FILED _____
1994	
GELES	

b6  
b7C

IN

DATE: 07/09/94 TIME: 18:26

MATCHED ON: \*L/N\*F/N

NAME: PETERSEN JUSTIN ADD: 374 CTY: SAN DIEGO

VR#: 11C5322 FC: M YR: 86 MK: HD

NAME: PETERSEN JUSTIN A ADD: 200 CTY: CHICO

\* VR#: 3HBD693 FC: A YR: 84 MK: CHEV

NAME: PETERSEN JUSTIN J ADD: 235 CTY: RAMONA

VR#: 2M14081 FC: C YR: 85 MK: MITS

VR#: 4H22400 FC: C YR: 85 MK: TOYT

ANI END

OUTPUT MSG 903, FROM CL2@ FOR FBI4 07/09/94 18:27

IN

DATE: 07/09/94 TIME: 18:27

MATCHED ON: \*L/N\*F/N\* MI

NAME: HEINZ ERIC E ADD: 170 CTY: SAN RAFAEL

VR#: 1CWA851 FC: A YR: 81 MK: VOLVO

VR#: J496992 FC: S YR: 35 MK: DP

ANI END

OUTPUT MSG 904, FROM CL10 FOR FBI4 07/09/94 18:27

(Indicate page, name of  
newspaper, city and state.)

(Mount Clipping in Space Below)

# Fugitive Hacker Leaves Trail of Strange Claims

■ **Crime:** 'Agent Steal' said he worked undercover for the FBI while awaiting sentencing for crimes that include rigging radio station contests. Case sheds light on shadowy computer world.

By JOHN JOHNSON  
TIMES STAFF WRITER

He called himself Agent Steal, computer hacker. He was a slender, good-looking rogue partial to Porsches and BMWs who bragged that he worked undercover for the FBI catching other hackers.

But today Agent Steal, whose real name is Justin Tanner Petersen, is on the run from the very agency he told friends was paying his rent and flying him to computer conferences to spy on the hacking community.

Petersen, 34, a Westside resident, disappeared in October after admitting to federal prosecutors that he had been committing further crimes during the time he claimed to be working with the government "in the investigation of other persons," according to federal court records.

His story is a microcosmic slice of the close-knit and ruggedly competitive world of computer hacking, where friends struggle to outdo each other and then, when they're caught, sometimes turn on each other.

Authorities say Petersen's list of accomplishments, known as "hacks," includes breaking into computers used by federal investigative agencies and tapping into a credit card information bureau.

Petersen, who once promoted after-hours rock shows in the San Fernando Valley, was involved in the hacker underground's most sensational scam: hijacking phone lines at Los Angeles radio station KPWR-FM to win contests with prizes ranging from new cars to trips to Hawaii. The mastermind of that scheme was another hacker, Kevin Poulsen, a.k.a. Dark Dante. Poulsen is awaiting sentencing in connection with the case, having already

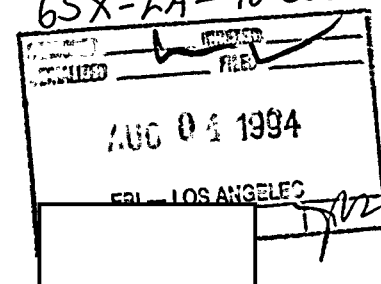
Please see HACKER, B4.

Date:  
Edition:

Title:

Character:  
or  
Classification:  
Submitting Office:

Indexing:



b6  
b7c

# HACKER: Fugitive's Trail of Strange Claims

-2-

Continued from B1

spent three years in custody, the longest term in jail for any hacker in history.

Petersen has boasted that he trapped former colleagues. Last year he gave an interview to an on-line publication called Phrack in which he claimed to have tapped the phone of a prostitute working for alleged madam Heidi Fleiss. He also bragged of working with the FBI to bust another infamous hacker, Kevin Mitnick, a San Fernando Valley man who has been hiding for almost two years to avoid prosecution for allegedly hacking into computers illegally and posing as a law enforcement officer.

"When I went to work for the bureau I contacted Mitnick," Petersen said in the Phrack interview. "He was still up to his old tricks, so we opened a case on him. . . . What a loser. Everyone thinks he is some great hacker. I outsmarted him and busted him."

Much of Petersen's story may be bunk. He is, after all, a shadowy person who didn't even use his own name during the years he spent on the fringes of the Los Angeles rock scene. Longhaired Eric Heinz, as Petersen called himself, shattered the computer nerd stereotype. He frequented the Rainbow Bar and Grill on Sunset Boulevard, often with different women on his arm, and handed out cards identifying himself as a concert promoter and electronic surveillance specialist.

The FBI refused to talk about Petersen directly. But J. Michael Gibbons, a bureau computer crime expert, said he doubted Petersen was working as a government informant to ensnare his hacker buddies for the bureau.

That kind of relationship is dangerous for the FBI, Gibbons said. "Across the board, hackers cannot be trusted to work—they play both sides against the middle." The agents "could have had him in the office," Gibbons said. "They probably debriefed him at length. [But] send him out to do things? I doubt it."

However, attorney Richard Sherman of Santa Monica, who represents another hacker, has accused the FBI of actively using Petersen as an informant and turning a blind eye to Petersen's alleged credit card fraud during the time he was in the bureau's care.

In a May 19 letter to Atty. Gen. Janet Reno, Sherman said three agents in Los Angeles engaged "in a course of conduct which is illegal and contrary to Bureau policy" in handling Petersen.

Jo Ann Farrington, deputy chief of the Justice Department's public integrity section, responded July 18 that there were no grounds to begin a criminal investigation. Assistant U.S. Atty. David Schindler in the Los Angeles office said, "It is factually incorrect that we allowed Mr. Petersen to commit crimes."

Those who knew Petersen best described him as a bright, verging-on-arrogant man who dressed well and sometimes walked with a cane, a result of a motorcycle accident six years ago that cost him a foot. He sometimes promoted after-hours clubs in the Valley and in Hollywood, according to a partner, Phillip Lamond.

Lamond said Petersen once told him: "The difference between you and me is I get a thrill from breaking the law."

In the Phrack interview, published on the Internet, an international network of computer networks with millions of users, Petersen, as Agent Steal bragged about breaking into Pacific Bell headquarters with hacker Poulsen to obtain information about the phone company's investigation of Petersen's hacking.

Petersen said they found "a lot of information regarding other investigations and how they do wire-

taps."

"Very dangerous in the wrong hands," said Phrack's interviewer, according to a transcript.

"We are the wrong hands," Petersen said.

Petersen was arrested in Texas in 1991, where he lived briefly. Court records show that authorities searching his apartment found computer equipment, Pacific Bell manuals and five modems.

An FBI affidavit expressed fear that Petersen could have been eavesdropping on law enforcement investigations. The affidavit said Petersen admitted "conducting illegal telephone taps" and breaking into Pacific Bell's COSMOS computer program, which allows the user to check telephone numbers and determine the location of telephone lines and circuits.

A grand jury in Texas returned an eight-count indictment against him, accusing Petersen of assuming false names, accessing a computer without authorization, possessing stolen mails, and fraudulently obtaining and using credit cards.

The case was transferred to California and sealed out of concern for Petersen's safety. The motion to seal, obtained by attorney Sherman, states that Petersen, "acting in an undercover capacity, currently is cooperating with the United States in the investigation of other persons in California."

Petersen eventually pleaded guilty to six counts, including rigging a radio station contest with a \$20,000 prize. He faced a sentence of up to 40 years in jail and a \$1.5-million fine, but the sentencing was continued several times. Sherman believes Petersen contin-

ued working for the government during that time. Petersen's partner, Lamond, said Petersen told him the FBI was paying him \$600 a month "to help them track down hackers."

On Oct. 18, 1993, 15 months after entering his first guilty plea, Petersen was confronted outside federal court by government attorney Schindler, who asked if he had been committing any crimes while on bail. Petersen said he had, according to Schindler.

Petersen then met briefly with his attorney and took off. "I've got a big problem and I'm splitting," he told a friend the same day.

Attempts to reach Petersen were unsuccessful and his attorney, Morton Boren, said he has "no knowledge of Justin committing any crimes."

Sherman also criticizes the government for allegedly allowing Petersen, while serving as an informant, to utilize a Pacific Bell Telephone Co. computer called Switched Access Services, known as SAS. Sherman said the computer allows operators to intercept telephone calls and place other calls, making it appear the calls originated from other phones.

Rich Motta, executive director of applications, reliability and support for Pacific Bell, said he would not comment on Sherman's allegations.

In the Phrack interview, Petersen made no apologies for his choices in life. Discussing Petersen's alleged role as an informant, interviewer Mike Bowen suggested that "most hackers would have done the same as you."

"Most hackers," Petersen replied, "would have sold out their mother."

U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

11000 Wilshire Blvd. #1700  
Los Angeles, CA 90024  
August 8, 1994

Dear Proprietor:

We are writing to you and other tanning salon proprietors in the Los Angeles area to ask for assistance in locating a fugitive suspect wanted by the FBI.

The fugitive, Justin Tanner Petersen, pled guilty to six felony counts in 1993. While on bail awaiting sentencing, he engaged in further criminal activity and his bond was immediately revoked. Petersen is believed to frequent tanning salons in the area. If you see Petersen, we ask that you do not confront him but rather call the FBI at (310) 477-6565, or your local police.

Petersen is described as a white male, age 34, 6-foot, 145-pounds with long brown hair and dark features. He is an amputee who wears a prosthetic lower left leg and is known to use a cane.

We ask that you and your employees carefully examine the enclosed roster of Petersen. You may call FBI Special Agent [redacted] at [redacted] (direct dial) with full confidentiality about information concerning Petersen's whereabouts. We appreciate any assistance you can provide in this matter.

Sincerely,

CHARLIE J. PARSONS  
Special Agent in Charge  
Los Angeles FBI Field Office

[redacted]

BY: [redacted]  
[redacted]  
Special Agent  
Los Angeles FBI Field Office

b6  
b7C

SEARCHED \_\_\_\_\_  
INDEXED \_\_\_\_\_  
SERIALIZED ✓  
FILED \_\_\_\_\_

65X-LA-12652-64/a

JMC



U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

11000 Wilshire Boulevard #1700  
Los Angeles, CA 90024  
August 10, 1994

Dear Proprietor:

We are writing to you and other prosthetic clinics in the Los Angeles area to ask for assistance in locating a fugitive suspect wanted by the Federal Bureau of Investigation (FBI).

The fugitive, Justin Tanner Petersen, pled guilty to six felony counts in 1993. While on bail awaiting sentencing, he engaged in further criminal activity and his bond was immediately revoked. Petersen is believed to visit prosthetic clinics for treatment in the area. If you see Petersen, we ask that you do not confront him but rather call the FBI at (310) 477-6565, or your local police.

Petersen is described as a white male, age 34, 6 foot, 145 pounds, with long brown hair and dark features. He is an amputee who wears a prosthetic lower left leg and is known to use a cane.

We ask that you and your employees carefully examine the enclosed poster of Petersen. You may call FBI Special Agent [redacted] at [redacted] (direct dial) with full confidentiality about information concerning Petersen's whereabouts. We appreciate any assistance you can provide in this matter.

Sincerely,

CHARLIE J. PARSONS  
Special Agent in Charge

[redacted]  
Special Agent

b6  
b7C

(indicate page, name of  
newspaper, city and state )

(Mount Clipping in Space Below)

# FBI Footwork Puts Computer Hacker in Jail

By JOHN JOHNSON  
TIMES STAFF WRITER

An FBI agent caught one of the nation's most wanted computer hackers in a foot chase Monday morning in West Los Angeles, where the fugitive was sighted about two blocks from the FBI's office after spending nearly a year on the run.

Justin Tanner Petersen, who has claimed that he worked undercover helping the FBI track down other criminal hackers, had been sought by federal agents since he fled while awaiting sentencing on a conviction stemming from the hacker underground's most sensational scam—hijacking radio station phone lines in Southern California to win contests with prizes ranging from new cars to trips to Hawaii.

Petersen also had pleaded guilty to tapping into the files of a credit card information bureau and transporting a

Please see HACKER, B4

Date: 8/30/94  
Edition: L.A. TIMES

Title

Character:  
or  
Classification:  
Submitting Office:

Indexing:

①

65X-LA-126522-65

SEARCHED	INDEXED
SERIALIZED	FILED
AUG 30 1994	
FBI - LOS ANGELES	

b6  
b7C

LOS ANGELES TIMES

## NEWS

## HACKER: Capture Follows Chase

Continued from B1  
stolen car across state lines.

A rangy, 34-year-old whose stylish clothing contrasted sharply with the stereotypical image of hackers as slovenly nerds, Petersen took the hacker moniker Agent Steal, using the name of an officer who once investigated him.

Petersen, who faces up to 40 years in prison and fines of up to \$1.5 million, was caught after a short foot chase that began outside an apartment building where an agent saw him getting out of a BMW, just blocks from the FBI's Westwood offices.

"It was superb police work by some very dedicated agents," said Assistant U.S. Atty. David Schindler, who would not reveal any other details of the capture.

Wearing open sandals, with dark hair down the middle of his back, Petersen appeared briefly before U.S. District Judge Stephen V. Wilson, who declined to set bail and scheduled sentencing Oct. 31.

Sentencing on the charges had been delayed several times while Petersen apparently cooperated behind the scenes—but never quietly—with the government's investigation of computer hacking.

Petersen told friends that the FBI was paying his rent and flying him to computer conferences to spy on other hackers. He gave an interview last year to an on-line publication called Phrack in which he claimed to have tapped the phone of Heidi Fleiss, the alleged "Hollywood madam." He did not say why.

He also bragged of helping the

FBI in their efforts to bust another hacker, Kevin Mitnick, the FBI's most wanted hacker suspect.

"When I went to work for the bureau I contacted" Mitnick, Petersen said in that interview. "He was still up to his old tricks, so we opened a case on him. . . . What a loser. Everyone thinks he is some great hacker. I outsmarted him and busted him."

Government agencies never have confirmed that they used Petersen as an active agent. The closest they have come is a reference in a federal court document that said Petersen, "acting in an undercover capacity, currently is cooperating with the United States in the investigation of other persons in California."

However close the relationship, it came to an end Oct. 22, 1993, when Petersen was confronted outside federal court and asked if he had been committing more crimes while awaiting sentencing on his other charges. Schindler said Petersen admitted he had.

After meeting briefly with his attorney, Petersen took off. "I've got a big problem and I'm splitting," a friend said Petersen told him the same day.

Petersen's attorney, Morton Boren, said he visited Petersen for a short time Monday at the Metropolitan Detention Center, where federal prisoners are held in Downtown Los Angeles. "He was depressed and worried," Boren said.

While he was on the run, friends continued to hear from him, and some said he never strayed far from his old Westside haunts. A

well-known figure on the nightclub scene who operated after-hours clubs in Hollywood and the San Fernando Valley, he had a reputation as a sharp dresser and ladies' man who sometimes carried a cane. He lost part of one leg in a motorcycle accident.

Schindler declined to say whether new charges will be filed against Petersen. At the time of his arrest, Petersen was carrying false identification, Schindler said.

Coincidentally, the alleged mastermind of the radio station contest scheme, Kevin Poulsen, who used the hacker nickname Dark Dante, was appearing in federal court Monday almost at the same time that Petersen was brought in. Schindler asked that a sealed plea agreement—in which Poulsen admitted computer fraud, obstruction of justice and money-laundering—be made public so the information could be used in Poulsen's upcoming Northern California trial on charges of possessing a national security document.

U.S. District Judge Manuel Real refused to make the agreement public, saying he did not want the case "tried in the press." He allowed Schindler to send the plea agreement to the judge in Northern California, who will decide whether the information contained in it can be used at trial.

Poulsen already has been in jail about 3½ years, the longest time spent behind bars by someone convicted of computer hacking crimes.

Times staff writer Julie Tamaki contributed to this story.

(Mount Clipping in Space Below)

# Computer criminal caught after 10 months on the run

By Keith Stone  
Daily News Staff Writer

Convicted computer criminal Justin Tanner Petersen was captured Monday in Los Angeles, 10 months after federal authorities said they discovered he had begun living a dual life as their informant and an outlaw hacker.

Petersen, 34, was arrested about 3:30 a.m. outside a Westwood apartment that FBI agents had placed under surveillance, said Assistant U.S. Attorney David

Schindler.

A flamboyant hacker known in the computer world as "Agent Steal," Petersen was being held without bail in the federal detention center in Los Angeles.

U.S. District Court Judge Stephen V. Wilson scheduled a sentencing hearing for Oct. 31.

Petersen faces a maximum of 40 years in prison for using his sophisticated computer skills to rig a radio contest in Los Angeles, tap tele-

See PETERSEN / Back Page

(Indicate page, name of  
newspaper, city and state.)

Page 1

Daily News, Van Nuys, CA

Date:

8-30-94

Edition:

Conejo Valley edition

Title:

FBI Agents Capture  
Computer Criminal

Character:

or

Classification:

Submitting Office:

Los Angeles

Indexing:

②

65-1A-126522

SEARCHED	INDEXED
SERIALIZED	FILED
AUG 31 1994	
FBI - LOS ANGELES	

b6  
b7C

**PETERSEN / From Page 1**

phone lines and enrich himself with credit cards.

Monday's arrest ends Petersen's run from the same FBI agents with whom he had once struck a deal: to remain free on bond in exchange for pleading guilty to several computer crimes and helping the FBI with other hacker cases.

The one-time nightclub promoter pleaded guilty in April 1993 to six federal charges. And he agreed to help the government build its case against Kevin Lee Poulsen, who was convicted of manipulating telephones to win radio contests and is awaiting trial on espionage charges in San Francisco.

Authorities said they later learned that Petersen had violated the deal by committing new crimes even as he was awaiting sentencing in the plea agreement.

The deal fell apart Oct. 22. Petersen admitted that he had not given up computer crime, but somehow managed to slip out of the federal courthouse in Los Angeles.

He then disappeared.

Several weeks ago, a man who identified himself as Petersen called the Daily News from an undisclosed location. Petersen's mother later confirmed the caller was him.

Petersen said he was living comfortably outside the United States and working as a bartender. He predicted he wouldn't be caught.

"I think I'll have to run for two

years. They'll stop looking for me, or it will slow down immensely," he said.

"It is annoying that I can't see old friends, I can't go to the Rainbow (Bar and Grill in Hollywood) and enjoy a lobster dinner at the front table," he said.

On Monday, FBI agents acting on a tip were waiting for Petersen when he parked a BMW at the Westwood apartment building. An FBI agent called Petersen's name, and Petersen began to run, Schindler said.

Two FBI agents gave chase and quickly caught Petersen, who has a prosthetic lower left leg because of a car-motorcycle accident several years ago.

Agent Stanley Ornellas was reluctant to discuss the case, except to say that when he caught Petersen, the computer whiz asked: "How did you find me?"

Schindler refused to provide additional details about Petersen's capture or where authorities believe the fugitive had been living.

It remains unclear whether Petersen will be charged additionally with fleeing custody and whether anyone will be charged with harboring a fugitive, Schindler said. Petersen was carrying identification for other people when he was arrested, he added.

"We know obviously there were people he was with," Schindler said.

In court, Petersen declined to comment, saying: "Mum's the

word." He was wearing prison-issue denims and did not appear to have changed his appearance while on the lam, except that his shoulder-length hair was brown rather than dyed blond, as it had been.

His mother, Joanne Dvorak, said she has been in contact with Petersen but did not know he had been arrested.

"If he needs me, I am here," she said. "Maybe this will be a blessing in disguise. Who knows — maybe he will get all straightened out.

"I just don't understand everything that is going on. Why do people do things like that? I just thought he was helping people — not doing bad things," she said.

Under Petersen's plea agreement, he faces a maximum prison sentence of 40 years and a fine of \$1.5 million and three years of supervised release.

Petersen's court-appointed attorney, Morton Boren, said he hopes the judge takes into account Petersen's cooperation with authorities.

In April 1993, Petersen pleaded guilty to six federal charges including conspiracy, computer fraud, intercepting wire communications, transporting a stolen vehicle across state lines and wrongfully accessing TRW credit files.

Among the crimes that Petersen has admitted to was working with other people to seize control of telephone lines so they could win radio promotional contests. In 1989, Petersen used that trick and walked away with \$10,000 in prize money

from an FM station, court records show.

When that and other misdeeds began to catch up with him, Petersen said, he fled to Dallas, where he assumed the alias Samuel Grossman and continued using computers to make money illegally.

In the summer of 1991 in Dallas, Petersen was pulled over driving a stolen Porsche and was arrested on charges that he had broken into credit bureau computers as part of a credit card scheme.

In the telephone interview several weeks ago, Petersen said his crimes victimized banks, not individuals.

"It wasn't losing any people any money. It was coming from the bank. I do have a conscience," he said.

"Computers have always been interesting to me, and if I can find a sneaky way to make a buck that is interesting and fun — that is fine," he said.

When he was finally arrested in 1991, Petersen said he played his last card.

"I called up the FBI and said: 'Guess what? I am in jail,' " he said.

He said he spent the next four months in prison, negotiating for his freedom with the promise that he would act as an informant in Los Angeles.

The FBI paid his rent and utilities and gave him \$200 a week for spending money and medical insurance, Petersen said.

They also provided him with a computer and phone lines to gather information on hackers, he said.

Petersen pointed agents to the location of Kevin Lee Poulsen's computer. Poulsen was convicted in June of rigging radio station telephones to win Porsches, cash and a trip to Hawaii.

Poulsen already has spent 3½ years in custody — more time than any other hacker — and now is awaiting trial in San Francisco on espionage charges that involve breaking into an Army computer network.

Coincidentally, on Monday a federal judge in Los Angeles denied a motion to unseal a plea agreement Poulsen had signed in the radio scheme conviction. But the judge allowed the agreement to be used in the San Francisco case if the judge there agrees.

Another computer hacker Petersen said he helped the FBI gather information on was Kevin Mitnick, a Calabasas man who was on probation for an earlier computer crime conviction.

Mitnick is a fugitive.

Eventually, Petersen said, the FBI stopped supporting him, so he turned to his nightclubs for income. But when that began to fail, he returned to hacking for profit.

"I was stuck out on a limb. I was almost out on the street. My club was costing me money because it was a new club," he said. "So I did what I had to do. I am not a greedy person."

# Memorandum

~~SECRET~~



To : SAC, LOS ANGELES (203C-LA-173258)  
(NSD-3) (P)

Date 8/31/94

From : TIS [REDACTED]

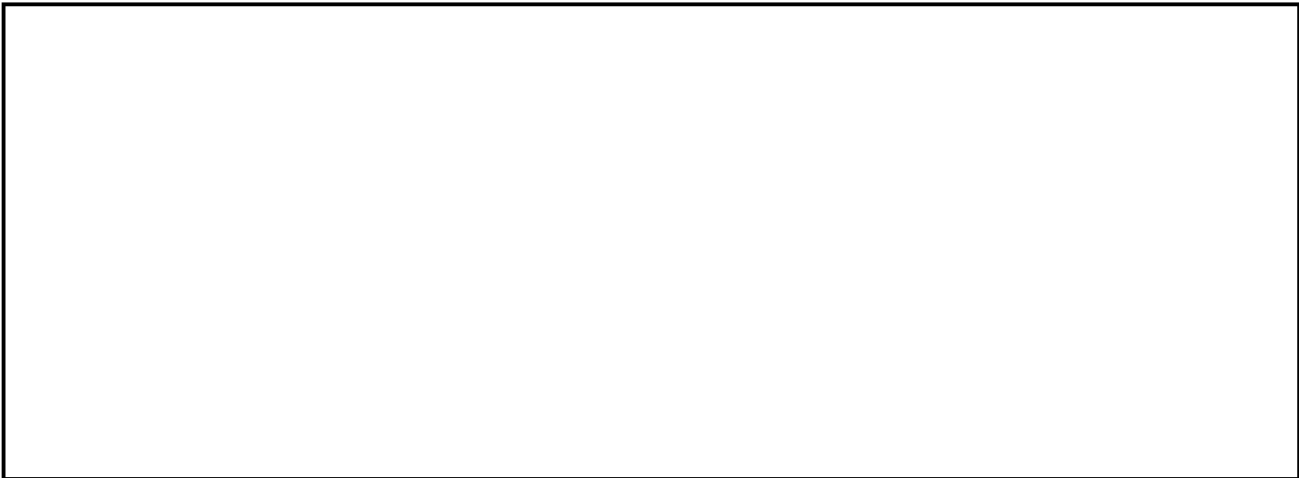
b6  
b7C

Subject: LEGION OF DOOM (COMPUTER CRIMES)  
FCI - CRITICAL TECHNOLOGY (X)  
OO: LOS ANGELES

This communication is classified "~~SECRET~~" in its entirety.

Reference the communication sent under this title on 8/16/94.

The Atlanta Division investigated the computer hacking group, the Legion of Doom (LoD), under file 65C-AT-62803. The following is a complete list of LoD members and associates which appear in the book The Hacker Crackdown, by Bruce Sterling, and/or were uncovered by Atlanta during their investigation:



(\*) = indicates a reference in Sterling's book.

b6  
b7C

- 1 - 203C-LA-173258
- ② - 65X-LA-126522
- 1 - SA [REDACTED]

~~CLASSIFIED BY: 9933~~  
~~DECLASSIFY ON: OADR~~

MAD/mad  
(4)

*File*

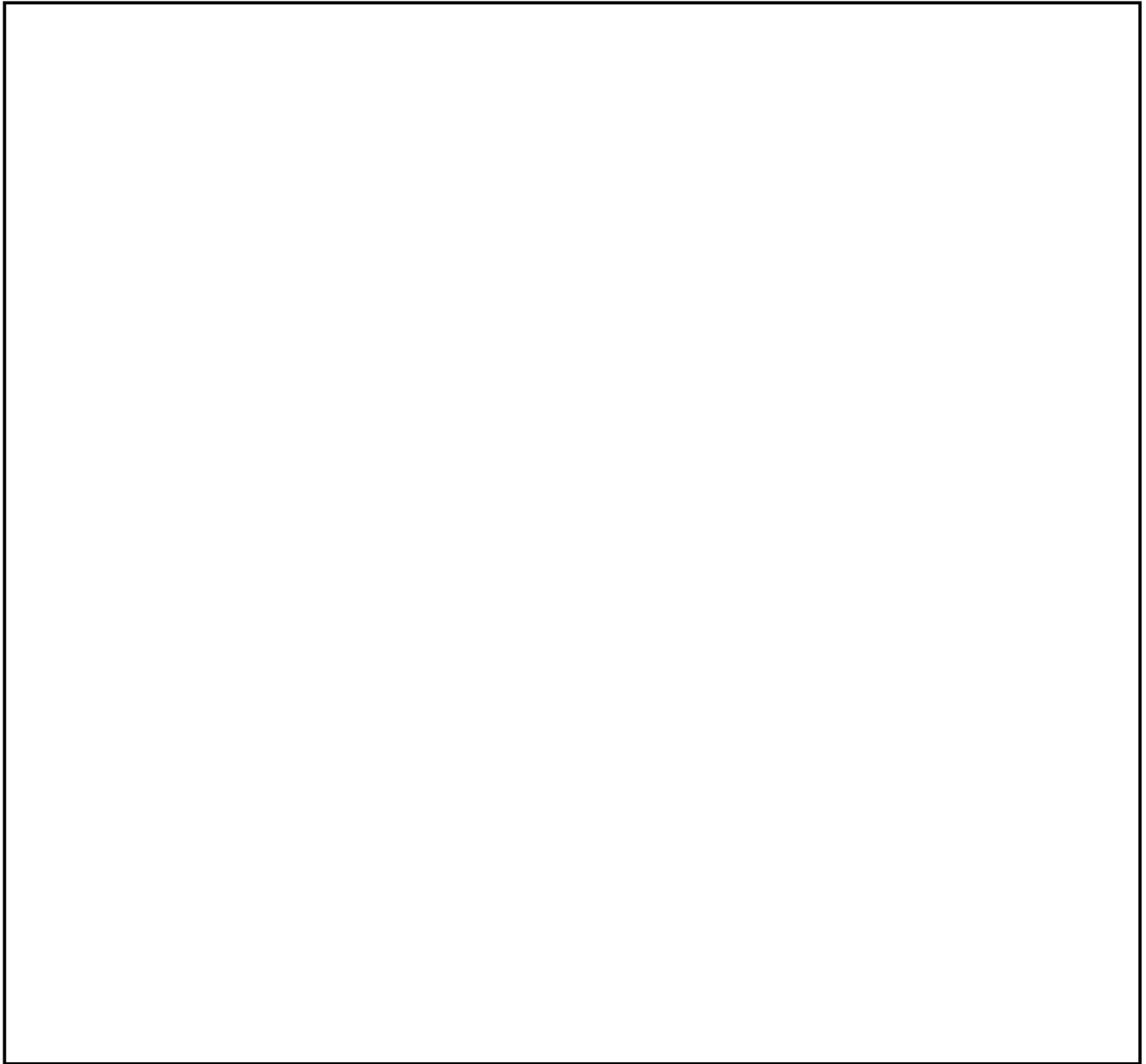
~~SECRET~~

65X-LA-126522

SEARCHED	INDEXED
SERIALIZED	FILED
AUG 31 1994	
FBI - LOS ANGELES	

~~SECRET~~

LoD Members (continued):



b6  
b7C

~~SECRET~~



~~SECRET~~

LoD Members (continued):

(Unknown), aka [redacted] (\*)

(Unknown), aka [redacted] (\*)

(Unknown), aka [redacted] (\*)

(Unknown), aka [redacted] (\*)

(Unknown), aka [redacted] (\*)

(Unknown), aka [redacted]

[redacted] (\*)

(Unknown), aka [redacted] (\*)

b6  
b7C

Known Associates of LoD:

(Unknown), aka [redacted]

(Unknown), aka [redacted]

(Unknown), aka [redacted]

[redacted]  
(Unknown), aka [redacted]

b6  
b7C

~~SECRET~~

~~SECRET~~

Known Associates of LoD:

(Unknown), aka [REDACTED]

b6  
b7C

Justin Tanner Petersen, aka "Agent Steal", aka "Phucked Agent 04". Subject of 65X-LA-126522. Said by Sterling to have been part of the original "hacker wing" of LoD. (\*)

The above listed names are being placed into this file for indexing into FOIMS [REDACTED]

b7E

~~SECRET~~

# Memorandum

DECLASSIFIED BY 60324 uc baw sab/ml  
ON 05-04-2011

~~SECRET~~



To : SAC, LOS ANGELES (203C-LA-173258)  
(NSD-3) (P)

Date 8/16/94

From : TIS [REDACTED]

Subject: LEGION OF DOOM (COMPUTER CRIMES)  
FCI - CRITICAL TECHNOLOGY (X)  
OO: LOS ANGELES

b6  
b7C

This communication is classified "~~SECRET~~" in its entirety.

Information relating to the computer hacking group "The Legion of Doom" (LoD) was obtained from the Atlanta Division as well as from the book, The Hacker Crackdown, by Bruce Sterling, and other open source publications.

According to Atlanta, the LoD was the subject of an espionage investigation conducted between 9/14/89 and 12/8/89 under file 65C-AT-62803. Three members of the LoD were charged with conspiracy to commit computer fraud, wire fraud and ITSP for their part in breaking into Bell South's computer network.

[REDACTED] plead guilty to charges of fraud and conspiracy according to a 7/10/90 Wall Street Journal article. [REDACTED]

b6  
b7C

[REDACTED] They were sent to a federal prison camp in Talladega, Alabama, for their crimes.

- 1 - 203C-LA-173258.
- ② - 65X-LA-126522
- 1 - SA [REDACTED]

~~CLASSIFIED BY: 9933  
DECLASSIFY ON: OADR~~

b6  
b7C

MAD/mad  
(4)

1-FILE COPY  
1-AGENT COPY

~~SECRET~~

65X-LA-126522-68

SEARCHED	INDEXED
SERIALIZED	FILED
AUG 16 1994	
FBI - LOS ANGELES	

mo

~~SECRET~~

The book The Hacker Crackdown states that [redacted] (identified as [redacted] by the Atlanta Division), formed the LoD when he was 18 years old who helped parlay a group of phone phreaks into computer hackers. "The LoD was built on the ruins of an earlier phreak group, The Knights of Shadow. Later, LoD was to subsume the personnel of the hacker group Tribunal of Knowledge. People came and went constantly in LoD; groups split up or formed offshoots.

b6  
b7C

"Early on, the LoD phreaks befriended a few computer-intrusion enthusiasts, who became the associated Legion of Hackers. Then the two groups conflated into the Legion of Doom/Hackers, or LoD/H. When the original 'hacker' wing, Messrs. 'Compu-Phreak' and 'Phucked Agent 04' (Justin Tanner Petersen the subject of 65X-LA-126522 and a fugitive from the FBI), found other matters to occupy their time, the extra '/H' slowly atrophied out of the name; but by this time the phreak wing, Messrs. [redacted]

[redacted] had picked up a plethora of intrusion expertise and had become a force to be reckoned with."

A hacker using the name [redacted] was also identified by [redacted] as an LoD member. [redacted] was a known computer associate of [redacted] who testified against LoD members during their 1990 trial. [redacted] had been raided by the U.S. Secret Service on 7/22/89 for their part in the computer hacking of BellSouth.

b6  
b7C

[redacted] also states, "There was no question that most any American hacker arrested would 'know' LoD. They all knew the handles of contributors to the LoD Tech Journal, and were likely to have learned their craft through LoD (electronic bulletin) boards and LoD activism. But they'd never met anyone from LoD. Even some of the rotating cadre who were actually and formally 'in LoD' knew one another by board mail and pseudonyms."

~~SECRET~~

~~SECRET~~

Atlanta identifies the Legion of Doom's primary members  
as:



b6  
b7C

~~SECRET~~

## News Chronicle

(Indicate page, name of newspaper, city and state.)

Thousand Oaks,  
California

Date:

3-28-95

News - P. 4

Edition:

Conejo Valley

Title: Computer Hacker Pleads Guilty  
to Fraud Charges

Character:

or

Classification:

Submitting Office:

Los Angeles

Indexing:

(Mount Clipping in Space Below)

# Computer hacker pleads guilty to fraud charges

By Keith Stone

Daily News Staff Writer

A computer hacker who admitted rigging radio station contests in Los Angeles pleaded guilty Monday to additional charges that he used his electronic skills to take \$150,000 from Glendale company in 1994.

Justin Tanner Petersen, 34, entered his guilty plea in U.S. District Court in Los Angeles to conspiracy to commit computer fraud and

committing wire fraud while he was a fugitive.

Petersen faces a possible maximum prison term of 60 years and \$2 million in fines. He is scheduled to be sentenced June 5 by Judge Stephen Wilson.

Assistant U.S. Attorney David Schindler said Petersen used his computer knowledge to illegally obtain passwords for Heller Financial Inc. in Glendale. On Aug. 17, 1994, Petersen entered Heller's computers and transferred

\$150,000 to Union Bank, Schindler said.

"He telephoned in two bomb threats on Aug. 17, the day the wire transfer occurred, in order to have the building cleared when the wire transfer was executed," Schindler added.

The money was sent to the account of an unnamed co-conspirator at the Union Bank branch in Bellflower, Schindler said. No charges have been filed against that person, but an investigation is under way, Schindler said.

On Monday, Petersen also pleaded guilty to illegally obtaining about 40 computer passwords belonging to Heller, the popular computer service America On-Line, and the credit company TRW.

Petersen's court-appointed attorney Morton H. Boren said Petersen is contrite. "I think Justin realizes he has a price he has to pay for what he has done," Boren said.

Investigators contend that Petersen committed the crimes just before his capture in Westwood in

August 1994. Known in cyberspace under the alias "Agent Steal," Petersen had been working with federal agents as an informant against other hackers.

But when agents discovered he also was using his computer skills to enrich himself, Petersen ran and led them on a chase that lasted 10 months.

Petersen also has pleaded guilty to seizing control of telephone lines to win cash prizes, cars and vacations in radio giveaway contests in Los Angeles.

65X-LA-126522-69

SEARCHED	INDEXED
SERIALIZED	FILED
MAR 29 1995	
FBI - LOS ANGELES	

LOS ANGELES

## Man Pleads Guilty to Role in Illegal Wire Transfer

Computer hacker Justin Tanner Peterson, who called himself "Agent Steal" and used his skills to obtain Porsches, trips to Hawaii and other luxuries, pleaded guilty to conspiring to cause a \$150,000 wire transfer.

Peterson, who was handcuffed as he appeared before U.S. District Judge Stephen V. Wilson, admitted that he conspired to transfer \$150,000 from a branch of Heller Financial Inc. in Glendale to the Union Bank account of an as-yet unidentified co-conspirator in Bellflower.

He also admitted illegally possessing 40 passwords from accounts at Heller Financial, TRW and America OnLine.

Assistant U.S. Atty. David Schindler said that to cover up their crime, the conspirators telephoned two phony bomb threats so bank employees would evacuate the buildings at the time the money was transferred.

Peterson, a tall, slender 34-year-old whose flowing hair and stylish manner of dress contrasted with the stereotype of the computer nerd, once worked as a promoter at after-hours clubs in Hollywood and the San Fernando Valley.

He gained notoriety in hacker circles when he and famed hacker Kevin Poulsen rigged phone lines at three radio stations and won two Porsches, two giveaways for \$20,000, one for \$10,000 and at least two trips to Hawaii, the prosecutor said.

Peterson's pleaded guilty on Aug. 29 to charges stemming from those giveaways.

His most recent crimes occurred between Oct. 22, 1993, and last Aug. 29, while authorities were searching for him. Peterson had skipped bail in the contest-rigging case, prosecutor Schindler said.

Peterson is scheduled to return to court June 5 for sentencing in both cases. Attorneys said that because federal sentencing guidelines are complex in this case, they are uncertain how much time Peterson might face. But the charges carry statutory maximum sentences of 60 years in federal prison and \$2 million in fines.

Peterson was captured last August following a brief chase just two blocks from the FBI's offices in West Los Angeles.

— ANN W. O'NEILL

LA TIMES  
3/28/95

*[Handwritten signature]*

1-FILE COPY

1-AGENT COPY

65x-LA-126522-70

SEARCHED	INDEXED
SERIALIZED	FILED
MAR 28 1995	
FBI - LOS ANGELES	

*[Handwritten signature]*

b6  
b7c

0023 MRI 00044

RR FBILA

DE FBILA #0007 1470216

ZNY SSSSS

R 270104Z MAY 95

FM FBI LOS ANGELES (65X-LA-126552) (C)

TO DIRECTOR FBI/ROUTINE/

BT

~~SECRET~~

CITE: //3410:FCI-3//

PASS: IOS [REDACTED] NSD.

b6  
b7C

SUBJECT: JUSTIN TANNER PETERSEN, AKA ERIC HEINZ; ESP-X  
(COMPUTER HACKING); OO: LOS ANGELES.

THIS COMMUNICATION IS CLASSIFIED "~~SECRET~~" IN ITS  
ENTIRETY.

[REDACTED]

AS FBIHQ IS AWARE, CAPTIONED SUBJECT WAS INVOLVED IN A  
SOPHISTICATED COMPUTER HACKING SCHEME WITH KEVIN LEE POULSEN  
IN LOS ANGELES, INVOLVING AMONG OTHER THINGS [REDACTED]

b7E

[REDACTED]

~~SECRET~~  
~~IIS-LOS ANGELES~~  
DATE 9/27/95  
REVIEWED BY [initials]  
ENTRY YES 2 NO NO  
IIS ENTERED Closed  
SERIAL(S) 63-72

65X-LA-126522-72

TELETYPE

SEARCHED \_\_\_\_\_  
INDEXED \_\_\_\_\_  
SERIALIZED lb  
FILED lb

RAH



PAGE TWO DE FBILA 0007 ~~S E C R E T~~

SUBJECT ALSO CONTINUES AS THE FOCUS OF A PARALLEL 139 CRIMINAL INVESTIGATION

ON OCTOBER 22, 1993, AS A RESULT OF INFORMATION RECEIVED, INDICATING THAT PETERSEN MAY HAVE BEEN INVOLVED IN ADDITIONAL CRIMINAL ACTIVITIES, HE AND HIS ATTORNEY APPEARED AT THE U.S. ATTORNEY'S OFFICE, LOS ANGELES, CALIFORNIA. [REDACTED]

[REDACTED]

b7D

[REDACTED] PETERSEN WAS ASKED IF HE HAD ENGAGED IN ANY CRIMINAL ACTIVITY WHILE OUT ON BAIL. SPECIFICALLY, HAD HE BEEN USING STOLEN CREDIT CARDS. PETERSEN ADMITTED THAT HE HAD IN FACT BEEN USING THE CREDIT CARDS OF OTHER INDIVIDUALS. AT THAT POINT IN THE CONVERSATION, PETERSEN ASKED TO SPEAK PRIVATELY WITH HIS ATTORNEY. PETERSEN AND HIS ATTORNEY INDICATED THAT THEY WOULD RETURN SHORTLY, HOWEVER, WHILE ALONE WITH HIS ATTORNEY PETERSEN FLED THE COURTHOUSE.

ON OCTOBER 22, 1993, U.S. DISTRICT COURT JUDGE STEPHEN WILSON REVOKED PETERSEN'S BOND AND ISSUED A BENCH WARRANT FOR PETERSEN'S ARREST, WHICH WAS EFFECTED SEVERAL MONTHS LATER.

SINCE THAT TIME, FBI LOS ANGELES HAS FOUND NOTHING IN THE DATA CONTAINED ON PETERSEN'S SEIZED COMPUTER THAT WOULD

PAGE THREE DE FBILA 0007 ~~SECRET~~

SUGGEST PETERSEN HAS BEEN ENGAGED IN ESPIONAGE. THIS MATTER IS  
CONSEQUENTLY BEING CLOSED. A NEW PLEA AGREEMENT HAS BEEN  
REACHED WITH PETERSEN, WHO IS NOW SCHEDULED FOR SENTENCING ON  
JUNE 5, 1995. INASMUCH AS THE CURRENT CASE AGENT HAS BEEN  
TRANSFERRED TO FBIHQ, THE RESULTS OF THAT SENTENCING WILL BE  
FORWARDED TO FBIHQ WITH A COPY FOR NSD UNDER THE 139 CAPTION.

~~C BY 9933; DECL ON OADR.~~

BT

#0007

NNNN

~~SECRET~~

(12/31/1995)

DATE: 04-27-2011  
CLASSIFIED BY 60324 uc baw sab/ml  
REASON: 1.4 (c)  
DECLASSIFY ON: 04-27-2036

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

~~SECRET~~

## FEDERAL BUREAU OF INVESTIGATION

**Precedence:** PRIORITY

**Date:** 03/12/1998

**To:** FBI Headquarters

**Att.:** AI

Room 5022;

IRS

**From:** Los Angeles  
NSD-3

**Contact:** SA [redacted] (310) 996-3557

**Approved By:** [redacted]

**Drafted By:** [redacted] :lmb

(U) **Case ID #:** ~~(S)~~ 66F-HQ-C1227695 (Pending)

(U) **Title:** ~~(S)~~ SHOT CLOCK;  
OO:FBIHQ

(U) **Synopsis:** ~~(S)~~ Los Angeles review of case file 65X-LA-126522, captioned JUSTIN TANNER PETERSON, A.K.A. ERIC HEINZ; ESP-X (Computer HACKING); OO:Los Angeles. Los Angeles response to FBIHQ E.C. dated 02/26/1998 as captioned, and assessment of potential damage to National Security if former FBI Agent [redacted] [redacted] compromised information provided to FBIHQ from 65X-LA-126522.

~~(S)~~ **Derived From :** G-3  
**Declassify On:** X-1

DUE TO SENSITIVITIES INVOLVED, DISSEMINATION OF THIS COMMUNICATION AND HANDLING OF THIS REQUEST SHOULD BE HANDLED ON A STRICT NEED TO KNOW BASIS. UNDER NO CIRCUMSTANCES SHOULD ANY INFORMATION CONTAINED HEREIN BE PROVIDED TO ANYONE OUTSIDE OF THE FBI WITHOUT PRIOR AUTHORIZATION FROM FBIHQ.

(U) **Reference:** ~~(S)~~ FBIHQ EC dated 02/26/1998, as captioned. Referenced communication was sent to FBIHQ ADP and Telecommunications Security, Infosystems Security Unit, and Security Countermeasures Section. Copies were also sent to Los Angeles and San Francisco. The EC contained nine interrogatives designed to elicit responses that would assist FBIHQ in providing a damage assessment for any activities [redacted] engaged in vis-a-vis 65X-LA-126522.

~~SECRET~~

65X-LA-126522  
closed -


73

~~SECRET~~

To: FBI Headquarters From: Los Angeles  
(U) Re: ~~(S)~~ 66F-HQ-C1227695, 03/12/1998

(U) Attachments: ~~(S)~~ Excerpts from "The Watchman".

(U) Details: ~~(S)~~ In response to the lead set forth in referenced EC, the Los Angeles response to interrogatives follows:



(S)

b1

~~SECRET~~

~~SECRET~~

b1  
b6  
b7C  
b7E

To: FBI Headquarters From: Los Angeles  
(U) Re: ~~(S)~~ 66F-HQ-C1227695, 03/12/1998

(S)

(U)

~~(S)~~ FBILA teletype to the Director, Dallas, Sacramento, San Francisco, and San Diego, (with direction to pass to SPU SSA [redacted] transmitted 08/07/1991, under FBILA file 65X-LA-126522 detailed the following compromises:

(S)

~~(S)~~ 1. [redacted]

(U) ~~(S)~~ 2. The methodology of how to compromise the [redacted]

(U) ~~(S)~~ 3. The ability and means utilized to [redacted]

~~(S)~~ 4. [redacted]

(S)

~~(S)~~ 5. [redacted]

(S)

b1  
b6  
b7C  
b7D  
b7E

~~SECRET~~

~~SECRET~~

To: FBI Headquarters From: Los Angeles

(U) Re: ~~(S)~~ 66F-HQ-C1227695, 03/12/1998

(U) ~~(S)~~ 6. Subjects could set up phone connections which give them the ability to monitor telephone lines from any location via phone modems. It is unknown if they did.

(S) ~~(S)~~ By teletype dated 08/16/1991, LA [redacted] 65X-LA-126522, transmitted to the Director, FBI, with pass line to SPU SSA [redacted]

(S)

b1  
b6  
b7C  
b7E

~~(S)~~ By teletype dated 03/09/1991, from San Francisco to the Director (pass to SPU SSA [redacted], Los Angeles, and Dallas, under FBILA file 65X-LA-126522, San Francisco advised FBIHQ of Security and FCI implications for the San Francisco Division as a result of information compromised by the subjects. Among the issues addressed by San Francisco are the following:

b6  
b7C

(U) ~~(S)~~ 1. San Francisco subject KEVIN POULSEN, an associate of Los Angeles subject JUSTIN PETERSON identified and contacted the subject of [redacted]

b7E

(U) ~~(S)~~ 2. POULSEN once physically surveilled a phone company circuit box used to connect [redacted]

b7E

~~(S)~~ 3. Circa 1987, POULSEN started sending e-mail communications which revealed an awareness of [redacted] and summarized Navy articles about the motivations for Americans to spy, voluntarily, for money. In 1987, subjects had amassed, through hacking, [redacted]

b6  
b7C  
b7E

[redacted] San Francisco. POULSEN and [redacted] POULSEN's hacking activity, surveyed the area around the Soviet Consulate looking for [redacted]

[redacted] They expressed interest in the

~~SECRET~~

~~SECRET~~

To: FBI Headquarters From: Los Angeles  
(U) Re: ~~(S)~~ 66F-HQ-C1227695, 03/12/1998

(S) subject of an FBI [redacted] operation where an Air Force enlistee volunteered classified information concerning the SR-71 to the Soviets.

b1  
b7E

(U) ~~(S)~~ 4. Through physical break-ins at telephone company locations [redacted]  
[redacted]

(U) ~~(S)~~ 5. During the period 1989-1991 POULSEN and PETERSON created documents [redacted]  
[redacted]

b6  
b7C  
b7E

(U) ~~(S)~~ By teletype dated 09/04/1991, transmitted to FBIHQ (pass to SPU SSA [redacted], Dallas, Sacramento, San Francisco and San Diego, under file 65X-LA-126522, Los Angeles advised the following:

(S) ~~(S)~~ 1. [redacted]  
[redacted]

b1  
b7E

(S) ~~(S)~~ 2. LA advised recipients of [redacted]  
[redacted]

(U) ~~(S)~~ 3. FBILA recommended [redacted]  
[redacted]

b7E

(U) ~~(S)~~ 4. FBILA recommended [redacted]  
[redacted]

~~(S)~~ By teletype dated 10/25/1991 to the Director, and Los Angeles, by San Francisco, under file 65X-LA-126522, San Francisco advised that San Francisco subjects POULSEN and [redacted] read in the newspaper of the FBI sting operation against [redacted] to volunteer to pass military secrets to the Soviets. They concluded this was [redacted]  
[redacted]

b6  
b7C  
b7E

[redacted] They broke into a San Francisco telephone company central office that they speculated serviced the consulate in an attempt to verify their theory, but were discovered by phone company employees and fled. In September, 1989, POULSEN visited

~~SECRET~~

~~SECRET~~

To: FBI Headquarters From: Los Angeles  
Re: ~~(S)~~ 66F-HQ-C1227695, 03/12/1998

[redacted] then in Los Angeles, and showed [redacted]  
[redacted]  
[redacted]

(S)

b1  
b6  
b7C  
b7D  
b7E

(S)

~~(U)~~ ~~(S)~~ By FBILA teletype to the Director, dated 06/08/1992, under file 268-HQ-1010175, subject [redacted] FBILA responded to a HQ tasking concerning countermeasures necessary as a result of the activities of PETERSON and POULSEN. This communication highlighted the following:

b6  
b7C  
b7E

~~(U)~~ ~~(S)~~ 1. Methodology used and a step by step process of how one could [redacted]

~~(S)~~ 2. The existence of hard copy printouts found among PETERSON'S belongings when he was arrested in Dalles, circa June, 1991. [redacted]  
[redacted]

(S)

b1

~~(U)~~ ~~(S)~~ 3. It contained recommendations as to preventative measures that could be taken to prevent future such discoveries (same as 09/04/1991 teletype discussed earlier).

~~(U)~~ ~~(S)~~ 4. No indications that PETERSON had provided information to a hostile service, [redacted]  
[redacted]

b1  
b7E

~~(S)~~ The foregoing is a summary of the information transmitted to FBIHQ concerning PETERSON and POULSEN and their computer hacking/phone company intrusions [redacted]

(S)

~~SECRET~~



~~SECRET~~

To: FBI Headquarters From: Los Angeles  
Re: (U) ~~(S)~~ 66F-HQ-C1227695, 03/12/1998

(S) [redacted] All of the foregoing was passed to FBIHQ  
during the period when [redacted] was at PSU. [redacted]

[redacted]

b1  
b6  
b7C

~~(S)~~ 1. [redacted]

[redacted]

(S)

~~(S)~~ 2. [redacted]

[redacted]

(S)

b1

~~(S)~~ 3. [redacted]

[redacted]

(S)

~~(S)~~ 4. [redacted]

[redacted]

(S)

b1

~~(S)~~ 5. [redacted]

[redacted]

(S)

(U) ~~(S)~~ 6. The FBI works with the phone company to  
facilitate telephone coverage.

(U) ~~(S)~~ 7. The ease to which a private individual could  
compromise the telephone company infrastructure, [redacted]

[redacted]

b7E

(U) ~~(S)~~ 8. [redacted]

[redacted]

~~(S)~~ [redacted]

[redacted]

(S)

[redacted]

b1

~~SECRET~~

~~SECRET~~

To: FBI Headquarters From: Los Angeles  
(U) Re: ~~(S)~~ 66F-HQ-C1227695, 03/12/1998

(S)

b1  
b7E

~~(S)~~ 3)

(S)

b1  
b6  
b7C  
b7E

~~SECRET~~

~~SECRET~~

To: FBI Headquarters From: Los Angeles

(U) Re: ~~(S)~~ 66F-HQ-C1227695, 03/12/1998

(U) ~~(S)~~ 6. Some [redacted]

b7E

POULSEN/PETERSON.

~~(S)~~ 4) [redacted]

(S)

[redacted] - San Francisco advised FBIHQ by teletype dated 03/09/1991, sent under file 65X-LA-126522 that San Francisco hacker KEVIN POULSEN had contacted the [redacted]

1987 he started expressing within his e-mail communications interests in [redacted] motivations for Americans to spy (monetary) and an interest [redacted]

b1  
b6  
b7C  
b7D  
b7E

[redacted] This same teletype also advised that POULSEN [redacted]

[redacted] There was no indication that POULSEN actually contacted the Soviets. In teletype dated 10/25/1991, from San Francisco to the Director, under file 65X-LA-126522, POULSEN'S actions [redacted]

[redacted] POULSEN [redacted] entered a telephone office they speculated might service the Soviet Consulate, but were forced to leave when discovered. In 1989, POULSEN showed [redacted]

b7E

(S) ~~(S)~~ Los Angeles found no evidence PETERSON had [redacted]

~~(S)~~ 5) [redacted]

(S)

b1

~~SECRET~~

To: FBI Headquarters From: Los Angeles

(U) Re: ~~(S)~~ 66F-HQ-C1227695, 03/12/1998

(S)

~~(S)~~ 6a)

(S)

b1

~~(S)~~

(S)

~~(S)~~ 7)

(S)

KEVIN POULSEN was the subject of a San Francisco investigation and was charged with espionage.

b1

~~(S)~~ 8)

(S)

~~(S)~~ 9)

(S)

- In addition to the information contained within this report, Los Angeles recommends that FBIHQ submit a lead to Denver to interview retired FBI Agent [redacted] former FBILA Security Manager. [redacted] resides in the Denver area and has telephone number [redacted] was contacted by SA [redacted] current FBILA Security Manager. [redacted] was contacted to assist LA in locating any documents relating to a damage assessment and for his recollections of events from the period of investigation of the hackers. [redacted] told [redacted] he had had numerous discussions with [redacted] about unrelated matters when [redacted] was at SPU. [redacted] contact with [redacted] was concerning various security related matters that [redacted] was involved with on a daily basis. The contact with [redacted] was of the nature of a Field Office

b1  
b6  
b7C

~~SECRET~~

~~SECRET~~

To: FBI Headquarters From: Los Angeles  
(U) Re: ~~(S)~~ 66F-HQ-C1227695, 03/12/1998

requesting advice and assistance from FBIHQ. [ ] was, at the time, in a position with SPU where [ ] could resolve issues or submit queries to [ ] for resolution or action. In this light, [ ] may have information on other matters relevant to [ ] of interest to FBIHQ.

b6  
b7C

~~(S)~~ Additionally, attached to this communication is a copy of pages from the book "The Watchman", by Jonathan Littman, published by Little Brown and Company, 1997. The attached extracts pertain to the actions of POULSEN and PETERSON, [ ]

(S)

b1  
b6  
b7C

(U) ~~(S)~~ Los Angeles POC is SA [ ], telephone [ ]

♦♦

~~SECRET~~

# THE WATCHMAN

THE TWISTED LIFE AND CRIMES OF  
SERIAL HACKER KEVIN POULSEN

---

JACOB H. LEE



LITTLE, BROWN AND COMPANY

Boston New York Toronto London

For Sherr

Copyright © 1997 by Jonathan Littman

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means, including information storage and retrieval systems, without permission in writing from the publisher, except by a reviewer who may quote brief passages in a review.

*First Edition*

Library of Congress Cataloging-in-Publication Data

Littman, Jonathan.

The watchman : the twisted life and crimes of serial hacker  
Kevin Poulsen / Jonathan Littman.—1st ed.

p. cm.

Includes index.

ISBN 0-316-52857-9

1. Poulsen, Kevin, 1965– 2. Computer hackers—United States—  
Biography. 3. Computers and society—United States.

4. Computer crimes—United States. 5. Computer security—  
United States. I. Title.

HV6772.P68L57 1997

364.16'8'092—dc21

96-47168

10987654321

HAD

Published simultaneously in Canada by Little, Brown  
& Company (Canada) Limited

Printed in the United States of America

the chain-link  
s long distan  
e parking  
distance cal  
nd Kevin can  
ne.

to me was  
mment about  
work early at  
r ten so I coul  
second", and  
couple hours

vening at the  
r balcony do  
aside, and un  
omb and wha  
ck at the tras  
cable. Kevin  
it down. He  
ns. Hand ove  
crete, twenty

en.  
ek they cras

entral offices, examining switches, perusing manuals, taking pass-  
ords and test trunk sets, collecting discarded Crossbars, once even pry-  
ing a pay phone off the wall. When Kevin's not inside Pac Bell's offices,  
he boots up his computer, turns on his modem, and roams the phone  
company's electronic ordering database—Cosmos, or Computer Sys-  
tem for Mainframe Operations. Studying those manuals he swiped has  
opened up worlds he didn't know existed. Kevin can do just about any-  
thing he wants in Cosmos: start or modify phone service, add or remove  
custom calling features, check for lines marked for repair, look up un-  
listed numbers. Kevin loves remote call forwarding or RCFs. For kicks,  
Kevin bounces calls around the Bay Area, trying to see how long a chain  
he can create.

Kevin and Gilligan fire e-mail back and forth, trading discoveries  
and comparing notes on everything from trunk lines and intricate Pac  
Bell calling options to tips on how to apply forty-eight volts to jolt the  
relays on their Crossbar switches to life. It's a strange mix of practical  
phreaking knowledge and phone trivia, the messages both giddy and  
conspiratorial, laced with reminders to call from a secure phone and  
bring tennis shoes and Levi's.

Kevin believes his adventures are innocent. This is the phone com-  
pany, after all, once the world's biggest monopoly. He can't imagine  
how his hobby could possibly threaten such a giant, powerful bureauc-  
racy. The phone company is practically invincible. He's just a kid swing-  
ing on the giant's shoelaces, going for a ride.

---

Gilligan lives near the San Francisco Soviet consulate, infamous for its  
satellite dish and forest of rooftop antennae aimed like ICBMs at Sili-  
con Valley. One of just three Soviet missions in the United States—the  
others are the embassy in Washington and the United Nations—the  
consulate is of huge strategic importance to the Soviet Union. The FBI  
estimates a third of the thirty-five- to forty-member delegation attached  
to the San Francisco consulate are intelligence officers. Against that  
cold war backdrop, Gilligan e-mails Kevin about how cool it would be  
to get a number similar to the Soviets' and snare some fascinating



wrong numbers. Then Gilligan follows up his message with a note about how reality seems to have anticipated his fantasy.

TO: KEV@SPAM.ISTC.SRI.COM  
SUBJECT: THE FBI  
DATE: 28 OCT 86 09:45:38 PST (TUE)  
FROM: GILLIGAN@SUN.COM (GILLIGAN GILLIGAN)

*It looks like the FBI had the same idea as I, but earlier. Did you hear on the news about this guy, a former Air Force enlisted man, who was arrested yesterday for spying? Well the news stories said that he phoned the Soviet embassy in San Francisco and told them that he had some secrets to sell. Unfortunately for this guy, the news story went on, the FBI "intercepted his telephone call" and staged a meeting with an undercover agent, who this guy mistook for a Soviet.*

*I wonder what kind of arrangement they have? The embassy phone number (922) is definitely in the [central] office that serves the area where the embassy is located. Perhaps the FBI just has the lines run through their offices and always acts as "receptionist" for the Soviets. I wonder what the entry for that line looks like in Cosmos?*

Obsessed, Gilligan drives by the consulate and urgently e-mails Kevin that all the windows on the first floor aren't windows at all but really one-way mirrors. But what intrigues Gilligan is how the FBI caught the spy. Does the FBI screen the Soviets' calls, and if so why wouldn't the Soviets catch on? Gilligan suggests the hackers find out for themselves.

"I think we should just give them a call and ask whoever answers who they are—FBI or embassy staff," Gilligan e-mails Kevin. "What do you say? We could do it on 3-way."

CORP

uth of Market :  
osing art deco s  
otham.

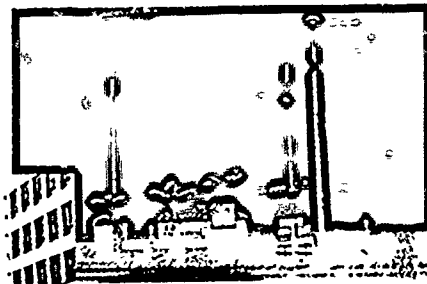
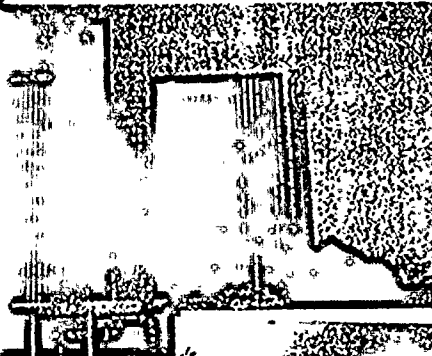
The date is Fel  
at will forever se  
electronic age.  
ak he's willing to  
orate headquarte  
floor and presses  
Kevin follows him  
talked it countless  
"G. S. Holt," he  
ook.

The guard han  
an suggested he t  
a sixth floor, sto  
city lights and  
ithin minutes, k  
"I'm in," Kevin  
Kevin takes hi

## FBI WIRETAPS HACKED BY KEVIN

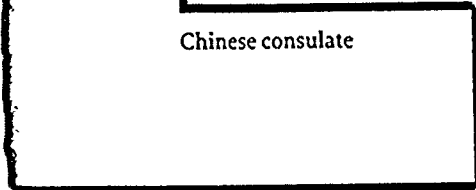
Kevin discovered the FBI was wiretapping foreign consulates and Ferdinand Marcos. He also discovered the site in the Los Angeles FBI headquarters building where many governments taps are monitored. The FBI was concerned about Kevin's discovery of taps in Concord, home of the Naval Weapons Station.

Los Angeles FBI headquarters

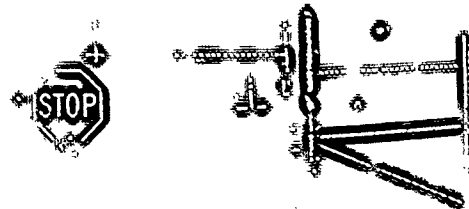


Israeli consulate

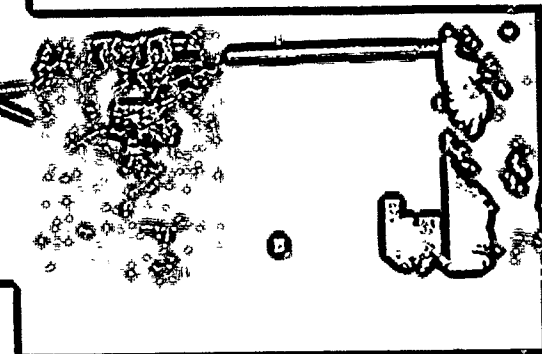
Chinese consulate



South African consulate



Concord Naval Weapons Station



Pac Bell office where Kevin discovered Ferdinand Marcos wiretap

Courtesy Bill Spradley

Courtesy Kurt Von Brauch

## TAP DANCING

Kevin sees what others don't.

When Eric spots the thin metal DNR tap lying on the floor of the Sunset CO, he only sees a hunk of steel connected to the frame. But Kevin looks beyond the physical discovery. He's interested in general principles, the greater framework. If he can understand how a single tap is placed perhaps he can understand others. Perhaps he can anticipate the taps he fears Pac Bell might place on the lines of his parents and friends.

So Kevin checks Cosmos and finds a clue. The on-line record does not—like a normal telephone number—include a cable pair assignment. From his apartment, Kevin dials Cosmos and begins searching for more of these unusual phone numbers. The first pass turns up over a hundred records, far too many taps for a single central office, and Kevin chastises himself for not anticipating the problem. Foreign exchanges, numbers that ring in one office and then run over a carrier to another office, don't show a cable pair, nor do remotely call forwarded numbers.

Kevin begins a crude search for every Pac Bell DNR tap in the state of California. When the sheer volume of the search bogs down in Cosmos, Kevin writes a program to streamline the process. Pac Bell's computers do his grunt work. His program runs on twenty Cosmos ma-

chines, half of them located in San Diego, the other half in Hayward, searching millions of telephone lines.

In just ninety minutes, Kevin Poulsen turns up roughly seven Pac Bell wiretaps spread around the state. He could visit the central office where each tap is located, to listen in, but he doesn't need to—he's got SAS. Kevin checks the first line. He hears a high-pitched tone, a signal to the phone company's tape recorders that the phone is on the hook and there's nothing to record. Then, the curtain of sound suddenly lifts, and he hears modem breath. Kevin watches someone upload a program to a bulletin board, then skips to a couple of other lines—a conversation, and more data transmission. He types a one-line description of what he finds on each tap.

Only Kevin knows exactly why he eavesdrops. The illicit taps are an obvious attraction for a hacker, but for Kevin maybe it's a question of survival, of checking the taps in case they lead back to him. Or perhaps something simpler, the allure of playing Jimmy Stewart in Hitchcock's *Rear Window*. Could Kevin have a higher goal? Might he be looking out for phone phreaks or others he believes are being unfairly targeted by the Phone Company? Whatever his motivations, that evening Kevin doesn't find anyone who merits his protection.

Each afternoon, Kevin searches the offices that switch Eric's, Ron's, his parents', and his own calls, canvassing every phone line in North Hollywood, Glendale, Sunset, Beverly Hills, and Van Nuys. He can begin hacking before his search is complete, because he knows how the system works. The records are entered into Cosmos a day or so before the technician physically hooks up the tap to the frame. It's a remarkable insight. The Watchman has developed the power to anticipate every Pac Bell wiretap in the state of California.

Kevin finds it in a B box on the street one night, a thin metal device with phone wires going in one end and out the other, and a big red sticker that warns, "Do not remove this device! Please call security at..."

Something tells Kevin this is different from the DNR tap he found

on Spiegel's line. At his apartment, he runs the circuit number listed on the device through Word, a Pac Bell system that tracks private circuit. "Please contact Mark Yelchak in security," says the file, giving an address of 180 New Montgomery. That's funny, Kevin thinks, remembering his late-night visit to Pac Bell's New Montgomery headquarters.

He pulls up the building in various Pac Bell systems, checking floor by floor. Something doesn't look right. Suddenly it hits him. The building he burglarized was 140 New Montgomery—not 180. Kevin zeros in on a single floor dedicated to security, a department called Electronic Operations, and finds fifty phone lines all grouped together. Electronic Operations—what could it mean? The files on each line contain a reference to the Pac Bell Computer Security System, and reveal the equipment on each line. Tape recorders. Fifty of them.

Kevin isn't totally surprised by his discovery. He knows that Pac Bell and other phone companies are required by law to carry out federal, state, and local court-ordered wiretaps. It's a carefully monitored legal process. The federal criminal code orders the assistant attorney general to "reveal the identity of the . . . law enforcement officer making the application . . . [and] make a . . . statement as to whether or not other investigative procedures have been tried and failed." Only specific crimes such as murder, espionage, kidnapping, racketeering, drug dealing, bribery, and fraud can justify taps. Even U.S. intelligence agencies have to apply to the Foreign Intelligence Surveillance Act court for national security wiretaps.

The Pac Bell taps Kevin has discovered appear to be DNRs which can double as wiretaps. That's what troubles Kevin. He knows there's nothing stopping Pac Bell from tapping dozens of lines on a moment's notice. Phone companies are the only entities in America that can wiretap with impunity, the only entities granted more power than the CIA, the NSA, or the FBI. The federal statute states that it is "not unlawful" for "an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service" to use that same service to "intercept . . . that communication" in the "protection of the rights or property of the provider of that service. . . ."

Somehow this doesn't make sense to Kevin. Other companies can't invade their customers' private conversations. Why shouldn't Pac Bell

and other phone law enforcement corporations?

But Kevin knows the statute is silent on traces and details wished to hide and could force it to reveal a number of thousands, fifty, or a thousand.

Kevin decides 180 New Montgomery ring endlessly or a SAS. If he hears a one-line summary.

Kevin repeats ninety minutes later the same figure he Cosmos taps scattered sees the same data Pac Bell tap has the office attached to Montgomery attached to System. Security enter a remarkable knows that if the ting there waiting the number plus

Kevin hasn't forgotten. He begins perusing finds another recording it to the first circuit domain numbers, the

number listed on private circuits, giving an address, remember headquarters. checking floor plan. The building Kevin zeros in on led Electronic Inter. Electronic contain a referral the equipment

as that Pac Bell try out federal, monitored legal attorney general making the appointment other investigation specific crimes drug dealing, agencies have it for national

DNRs which knows there's in a moment's that can wire-tap than the CIA, not unlawful" or agent of a use that same section of the

companies can't didn't Pac Bell

and other phone companies turn their fraud cases over to the proper law enforcement agencies, and let justice take its course, like other corporations?

But Kevin knows that the taps are only the tip of the iceberg. The statute is silent on the right of phone companies to perform taps and traces and detailed analyses of a suspect's calling patterns. If Pac Bell wished to hide an investigation from the FBI or Secret Service, no court could force it to reveal the nature or target of its inquiry. Even the annual number of taps is secret. Does Pac Bell wiretap ten people a year, fifty, or a thousand?

Kevin decides to find out. First he dials the fifty phone numbers at 180 New Montgomery and discovers that no matter what the hour they ring endlessly or are forever busy. Then he wiretaps all fifty lines with SAS. If he hears anything—conversation, modem tones—he writes a one-line summary. He comes up with seven working taps.

Kevin repeats his statewide Cosmos Pac Bell wiretap search, and ninety minutes later he can't believe what he's found. Seven numbers, the same figure he found in 180 New Montgomery. He drops in on the Cosmos taps scattered around the state and hears the same voices and sees the same data. It's as if he's stumbled onto a parallel universe. Every Pac Bell tap has two different monitor lines, one in the local central office attached to the suspect's line and another at 180 New Montgomery attached to a tape recorder and the Pac Bell Computer Security System. Security investigators can dial any of those fifty numbers and enter a remarkably easy one- to eight-digit security code. And Kevin knows that if the monitor line happens to be down the tap will be sitting there waiting to be exploited. Kevin won't even need SAS. Just dial the number plus the security code and wiretap the wiretapped.

---

Kevin hasn't forgotten about Mark Yelchak at 180 New Montgomery. He begins perusing random circuits on-line, and after a little checking, finds another record that suggests he contact Yelchak. Kevin compares it to the first circuit he found in the B box. Both are identified by two random numbers, then the letters AFLA, followed by a string of random

digits. That isn't all the two circuits have in common. Both originate in ordinary B boxes and terminate at 11000 Wilshire, the federal building, Los Angeles headquarters for the FBI. After further study, Kevin finds a couple of alarm pairs that don't run to the Federal building but share the AFLA designation. Kevin can't explain the false positives, but then he doesn't really need to: over 90 percent of the AFLA circuits he finds are federal wiretaps.

What surprises Kevin is how easy the federal government makes it to crack their vaunted veil of security. Since the early days of Hoover, wiretaps have been the secret weapon of the FBI, powerful enough to ensnare gangsters and keep political enemies and presidents in check. Indeed, traditionally wiretaps have been what separates the government from the crooks. The idea that an ambitious hacker with a PC could expose federal taps is absurd. If that's all it takes, then how well could the FBI be expected to investigate mobsters, corrupt politicians, and spies?

But as Kevin learns more about how the government and Pac Bell track federal wiretaps, he discovers that it's even worse than he thought. The Bureau is not the only federal agency that permits Pac Bell to track its taps on-line. Kevin soon finds taps running to two occupants of the Los Angeles World Trade Center, the DEA and the Secret Service—the primary federal agency entrusted with investigating hackers. And when Kevin enters "AFLA" circuits into another Pac Bell system to find out who ordered them, he finds that federal agents may actually have a sense of humor. "Acme" and the "Busy Bee" answering service order lots of federal wiretaps.

Being curious, Kevin sometimes wants to know who's being tapped. He could find the actual B box on the street, pry it open, and trace the wires from the metal federal tap to the binding post and the specific cable and pair numbers. Then, with Cosmos, he could turn the cable and pair into a phone number that could be entered into other systems to reveal the person's name, social security number, birthdate, driver's license, and finally the street address.

But Kevin checks few taps this way. Why rely on physical crutches if he can hack the answer? Many of the federal taps are in the San Fernando Valley, and Kevin sets out to learn why. Since Pac Bell's comput-

ers volunteer  
of the busines  
urance com  
tag, the comp  
ornography.  
nando Valley

Kevin can  
apartment. H  
shoes, then c  
within the tan  
ing on the fed  
phone numbe  
wished to, list

Why shou  
pursue him, v  
Kevin has to  
massive hole  
ment holds in  
founding fath  
it, they inste  
less searches  
counter any g  
corrupt.

Once a day  
checking doz  
an hour, the  
eign agents v  
FBI wiretap  
in the Union,  
of the most ac  
simply know  
and subscrib  
day it receive  
fore the taps  
power to cor  
cret Service.

both originate in  
federal building,  
y, Kevin finds a  
lding but share  
itives, but then  
ircuits he finds

ment makes it  
lays of Hoover,  
rful enough to  
dents in check.  
es the govern-  
ker with a PC  
then how well  
upt politicians,

at and Pac Bell  
vorse than he  
ermits Pac Bell  
two occupants  
the Secret Ser-  
gating hackers.  
Bell system to  
s may actually  
ring service or-

s being tapped.  
.. and trace the  
ad the specific  
n the cable and  
r systems to re-  
ate, driver's li-

ysical crutches  
in the San Fer-  
Bell's comput-

ers volunteer the B box of the tap, Kevin systematically checks the lines of the businesses within the building or block. Most appear ordinary: insurance companies, accountants, and lawyers. But then there's a red flag, the company name for what seems to be a publisher or producer of pornography. It makes sense. Los Angeles, and specifically the San Fernando Valley, produces much of the world's pornography.

Kevin can definitively locate the porn tap without ever leaving his apartment. He can remotely tap the tapped line in the B box with SAS shoes, then dial the suspected porn business or call every number within the target building. The proof? The sound of his own phone ringing on the federally tapped line—through his own tap. He'd have the phone number of the target of a federal investigation, and could, if he wished to, listen in.

Why should the government hold all the cards? If they're going to pursue him, why shouldn't he be able to track their moves? That's why Kevin has to take it further and write the program that will blast a massive hole in whatever false sense of security the federal government holds in its ability to play Big Brother. And really, why not? The founding fathers didn't promote spying in the Constitution. Far from it, they instead wrote the Fourth Amendment, prohibiting warrantless searches and seizures, and emphasized the right to bear arms to counter any government that might one day prove unrepresentative or corrupt.

Once a day, Kevin's computer polls the Southern California systems, checking dozens of central offices at a time. Each day, in a little over half an hour, the computer accomplishes a task for which the mob or foreign agents would gladly pay thousands of dollars. Kevin knows every FBI wiretap in Southern California, more than half of the largest state in the Union, boasting the sixth largest economy in the world, and some of the most advanced, classified technology in the nation. Kevin doesn't simply know the existing wiretaps. Pac Bell enters the circuit identifier and subscriber information, such as "Acme," into its computers the very day it receives a federal court order. But it's often days or even weeks before the taps are installed, days or weeks in which Kevin holds the power to compromise the moves of the FBI, the DEA, or even the Secret Service.



Who could possibly be wiretapping thirteen lines?

Kevin has found a building with thirteen taps, far more taps than he's ever found clustered in one location. Publicly, the FBI claimed that it wiretapped less than 250 people the previous year. How then could there be thirteen wiretaps focused within a single building in Beverly Hills?

Few federal judges would authorize thirteen wiretaps on a single individual or business. Even the biggest mob investigations seldom reach that size. No, Kevin has hit on something larger. Excited, he learns that the thirteen lines are being monitored from the federal building. He traces the tap back to its target, a process that is now second nature. At first, the Beverly Hills address means nothing to him. What could be so interesting across the street from the Beverly Center, the posh shopping mall for movie stars, celebrities, and the rich?

Not more than a few hundred feet from the shopping center stands the South African consulate. Could it really be true?

Ron punches up South Africa in Nexis, and watches the stream of stories mentioning nuclear power leap from the screen. The two hackers are dumbfounded. They've stumbled onto real life, honest-to-God spy taps, the stuff of espionage and national security. Kevin and Ron can't possibly know whether the taps are authorized under the Foreign Intelligence Surveillance Act by the Washington, D.C., court that grants taps to the CIA and other spy agencies. Unlike common FBI and state and local wiretaps, the court authorizations for spy taps have, according to the Justice Department, never been made public. But what the hackers have uncovered stuns them. Pac Bell's own on-line, Net accessible records provide irrefutable evidence the spy taps have been in place for several years.

It's just the beginning. Kevin finds ten more wiretaps that run back to the federal building, ten wiretaps in the Los Angeles consulate of our friendly ally Israel. And there's more. Incredibly, Kevin uncovers four-

teen taps in  
Wilshire a  
gence oper  
ties Union  
ing and fir  
match, so h  
consulate,  
from the A  
stead of run  
the Chinese  
downstairs  
office?

The gar  
world of in  
taps anywh  
step to exte  
tially, overs  
icans, the Isr  
the Israelis  
think about  
might it thi

Ron ph  
telligence f  
tends to be  
seem to get  
ness, the ne  
formation b  
the compar  
a large, whi  
dilapidated  
he's being v  
chandelier  
second floo  
he's in the

The offi  
of the cons

more taps than  
I claimed that  
ow then could  
ling in Beverly  
son a single in-  
s seldom reach  
he learns that  
il building. He  
ond nature. At  
hat could be so  
posh shopping  
center stands  
stream of sto-  
re two hackers  
est-to-God spy  
and Ron can't  
Foreign Intel-  
rt that grants  
FBI and state  
ave, according  
what the hack-  
Net accessible  
en in place for  
that run back  
nsulate of our  
uncovers four-

teen taps near an office of the American Civil Liberties Union around Wilshire and Sixth Street. Could one of the biggest FBI counterintelligence operations in Los Angeles be targeting the American Civil Liberties Union? Kevin checks all the businesses within the ACLU's building and finds one with five lines and another with two. There's no match, so his hunch about the ACLU must be wrong. But the Chinese consulate, on Shatto Street, off Wilshire, three doors down the street from the ACLU, has fourteen lines. And something else is unusual. Instead of running back to the federal building like the other foreign taps, the Chinese taps loop, jumping up to another floor, and then dropping downstairs. Could the feds be listening to the Chinese from an upstairs office?

The game of hacking has suddenly drawn Kevin into a dangerous world of international espionage. He can systematically ferret out spy taps anywhere in Southern California, and he knows that it's a small step to extend that capability to the rest of the nation, and even, potentially, overseas. Kevin could send evidence of the taps to the South Africans, the Israelis, the Chinese, or even the *Los Angeles Times*. What might the Israelis think about the ten wiretaps? And what might the FBI think about its secret taps being featured on the evening news? What might it think about a couple of hackers delving into national secrets?

Ron phones the number Kevin has dug up for the FBI's counterintelligence front operation at the Chinese consulate building and pretends to be looking for a job. The spies at J. W. Collins & Associates can't seem to get their story straight. One day they're in the publishing business, the next they're in the information business. What side of the information business J. W. Collins & Associates pursues is not something the company cares to discuss. Ron decides to pay a visit to the consulate, a large, white office building. As he gets out of his car he notices some dilapidated apartments across the way, and has the uneasy sensation he's being watched. He strolls through the marble lobby, past the cheap chandelier and half-dozing security guard, and takes the elevator to the second floor. A laminated plaque next to the tall brown doors tells him he's in the right place, J. W. Collins & Associates.

The office is larger than he imagined, covering nearly half the floor of the consulate's building, and resembling a law firm. Magazines are

neatly arranged around the chairs and table in the waiting room, and Ron can see numerous Macintosh computers and desks beyond. The only crack in the FBI's counterintelligence facade is the absence of people during normal business hours. Nobody seems to be home. The woman comes out after quite some time, a little old lady right out of the pages of a John le Carré novel.

"Can I help you?"

ting room, and  
s beyond. The  
absence of peo-  
be home. The  
right out of the

## KEVIN'S COURT

M  
alibu?

Kevin's found his first wiretap in the coastal home to Hollywood's stars. As he investigates further, he notices that the Malibu tap runs to a regional FBI office in Van Nuys. Why, Kevin wonders, is this tap running to a small office, situated farther from the tap than the federal building?

This time Kevin sees no easy method to divine the subject of the federal eavesdropping. SAS doesn't work with GTE, which handles service in Malibu. So how can he do it? The easiest method would be to drive out to the actual B box in Malibu and physically trace the lines, but Kevin keeps his actions secret. All Ron knows is that Kevin discovers that along with the FBI field office, a nearby Malibu residence has been set up as a listening post, and to add to the mystery, the subject of the wiretap appears to be a tony restaurant on the edge of the Pacific.

Why would the feds take such elaborate security measures for a restaurant? Ron searches the restaurant's name in Nexis and a story begins to unfold. An October 1988 *L.A. Times* article describes a Prudential Bache executive who "accepted a \$2 million post-dated check from ZZZZ Best carpet-cleaning kingpin Barry Minkow after he flew her to Los Angeles" and "took her out for an intimate seaside dinner . . . at Malibu's Splash restaurant."

Kevin and Ron, like just about everybody in Los Angeles, remember the ZZZZ Best scandal. The story became a parable for the greedy eighties, an improbable tale of a kid who seduced Wall Street and bilked thousands of investors with a carpet-cleaning pyramid scheme. But how does Splash fit in? And why would the feds still be tapping the joint long after Minkow had been exposed? Another article describes Splash's manager as Ronnie Lorenzo, "a member of the New York-based Bonnano crime family" and then names prominent New York mafiosos who frequented Splash and muscled in on the ZZZZ Best scam.

Kevin has hacked his way into one of the most publicized scams of the last two years, a national front-page story that led to congressional hearings. The federal attention and media circus only highlights Kevin's phenomenal find. Advance knowledge of federal wiretaps is indeed a powerful tool, and the more Kevin thinks about it, the more he realizes how fortunate it is that he's continued his vigilance against Eric. Eric already works for a detective who has no scruples about illegal wiretaps. What would stop Eric from offering his services to the mob to uncover federal wiretaps? Kevin knows it's not a hypothetical question. Although Minkow's in jail, the Splash tap is still live. Very live. Incredibly, within weeks of Kevin's discovery, Ronald Lorenzo, the owner of the trendy Malibu nightspot, begins having a series of phone chats with one Robert Franchi, an undercover FBI agent, over the very same line Kevin knows is being tapped by the FBI.

---

Kevin makes the seven-hour drive to Northern California to visit Lottor and Gilligan, but it's a little too long for his oil-leaking clunker. Just short of the Menlo Park exit, the engine seizes and the car dies on the freeway. Lottor isn't at his condo when he straggles in, and without a car Kevin wonders how he'll pass the afternoon. Then he remembers. There's a tap in the neighborhood he could check.

Kevin doesn't have long to wait before a white van pulls up to the B box. The driver, wearing a suit and a tie, doesn't look like a Pac Bell technician. Kevin sits on the wall near the 7-Eleven and sips the Coke he just bought. The man looks at Kevin and Kevin looks back. Even from a dis-

...eles, remember  
the greedy eighth  
street and bilked  
id scheme. But  
apping the joint  
article describes  
New York-based  
New York mafiosos  
st scam.  
icized scams of  
congressional  
nly highlights  
l wiretaps is in-  
it, the more he  
gillance against  
es about illegal  
s to the mob to  
etical question.  
ry live. Incred-  
o, the owner of  
one chats with  
very same line

a to visit Lottor  
g clunker. Just  
car dies on the  
d without a car  
ie remembers.

alls up to the B  
a Pac Bell tech-  
ie Coke he just  
ven from a dis-

tance, Kevin sees him carry the six-inch-long metal tap from the van. He can't quite make out the rest, but he can guess the routine. The man will connect the eavesdropped line to one end and the federal line to the other, lock the box, and be on his way. Kevin knows it's almost certain the box holds a federal tap: the FBI is about the only entity that bothers to lock B boxes.

Finally, after all his years as a hacker, Kevin has witnessed the placing of a federal tap. But far from being impressed, he's amused at what seems an amateur process. By its own count, the Bureau taps fewer than a few hundred people a year. So if the FBI considers the subject of the tap important enough to merit surveillance, why does it execute the final physical connection with all the subtlety and secrecy of Maxwell Smart?

---

Tucked away behind the hills east of Oakland, Concord draws Bay Area professionals for its warm weather, open space, and outdoor concerts. Kevin's heard of Concord, but it's always seemed sleepy. That's why he's surprised to find that the suburban community is home to a hotbed of FBI wiretaps.

A Nexis search would open his eyes to another side of the East Bay community. Concord is also home to the Concord Naval Weapons Station, the major West Coast supply center for military weapons and ammunition. Numerous reports, never confirmed by the military, say the station houses nuclear weapons. During the 1980s, the station became a trigger point for demonstrations about arms shipments to Central America. Antiwar demonstrators believed an elite FBI counterterrorist unit at the Concord office was specifically tracking one of the leading protesters. Brian Wilson, a former Vietnam Air Force Intelligence officer, had learned that the station shipped deadly white phosphorus explosives to El Salvador.

Then, in September of 1987, a terrible "accident" at the weapons station raised an international stir. Wilson lost both legs trying to block a train carrying munitions for the Contras and was declared a "courageous peace fighter" by Soviet newspapers. A fired FBI agent told the

*L.A. Times* that the Bureau considered Wilson a terrorist, engaged in a "violent conspiracy" against the government. Congresswoman Barbara Boxer demanded to know why the Navy train didn't stop. Was it an unavoidable accident? Or was the fired FBI agent correct that the Bureau considered Wilson a terrorist? And could the FBI have tapped the phones of Wilson and other protesters?

---

Kevin is more secretive about the Concord taps than he's ever been before, this time mentioning nothing to Ron and encrypting his files several times. Whether Kevin is alerting any of the targets of federal surveillance is hard to know. He has the tools and the knowledge, but it's not simply a technical question. Kevin weighs who he believes is deserving. If he encounters a hacker he deems worthy Kevin feels he has no choice but to warn him of the surveillance.

One evening, Kevin discovers a tap at 180 New Montgomery and listens to Shadow Warrior and a friend, a couple of young hackers toying with internal phone company test numbers and computers that respond in synthesized voices. Kevin takes to them immediately and decides they must be warned, but he can't just break in and say Dark Dante is coming to the rescue. Kevin prizes his ability to find taps for his own protection. How can he warn the hackers without clueing Pac Bell into his knowledge?

Just then, Shadow Warrior's friend three-ways off to listen to the synthesized voice of a credit card approval system.

"APPROVED FOR FIFTY DOLLARS," booms the staccato voice, and then mechanically reads off a phone number. The credit card system performed an ANA, an automatic number announcement check, and spat back the kid's phone number.

This is my opportunity.

Kevin punches the number on his test set.

"Oh shit," says the friend as his call waiting beeps. "Should I answer it?"

"Yeah! Answer it! Answer it!" shouts Shadow Warrior.

But his friend chickens out. "Oh shit, now I'll never know."

t, engaged in a  
Roman Barbara  
Was it an un-  
at the Bureau  
ve tapped the

s ever been be-  
ig his files sev-  
of federal sur-  
ledge, but it's  
believes is de-  
in feels he has

omery and lis-  
ackers toying  
uters that re-  
ately and de-  
y Dark Dante  
s for his own  
g Pac Bell into

listen to the

taccato voice,  
edit card sys-  
ement check,

ould I answer

ow."

Don't worry, you'll get a second chance.

Kevin waits a minute, then punches redial. This time the phone picks up the call. "Yeah right!" Kevin swaggers, trying to sound like a cop. "We know all about you and your buddy Shadow Warrior, and you'll be hearing from us soon."

Kevin is surprised by his emotions. His voice shook a little as he alerted the kid to the tap. He hangs up and eavesdrops on Shadow Warrior's monitor line.

"Oh shit, what was that?" the friend frantically asks Shadow Warrior.

"What happened?" asks Shadow Warrior.

"This guy!" exclaims the friend. "Man, he was serious business!" And then the conversation slips into what sounds like code. They seem to have gotten the point. They start talking about meeting somewhere. Kevin doesn't need to listen anymore.

The Watchman has done his part.

---

But Kevin's duty is not only to warn those being targeted by the phone company. When necessary, he taps his own enemies.

"I don't want to talk to you anymore, I don't want to hear from you anymore!" Eric declares in an unusually stiff, angry voice mail to Kevin not long after Kevin spooked him from Sunset. "We're finished because you tried to mislead me from valuable access! You should forget that I exist! Any attempts to locate my whereabouts will not be tolerated!"

Kevin has a quick retort: "I'll be happy to forget you existed provided that no evidence of your existence is forced upon me." But a few weeks later, while combing Pac Bell's on-line security memos, Kevin finds what he believes to be damning evidence of Eric's existence. Months before, not long after the three met, an anonymous tipster asked for Steve in the security department, and said an L.A. hacker had cracked the BANCS network at Pac Bell's San Ramon offices. "I also am a hacker in Los Angeles," the memo quoted the tipster, and then noted, "the caller sounded young."

Kevin calls Ron for an emergency meeting. Ron is his court, his mag-



istrate, and Kevin rarely taps without his approval. Kevin formally presents his evidence, an official computer printout of Pac Bell's security memo, and makes his argument that Eric must be the rat. "See how it mentions both the intruder and the tipster are from L.A."

Ron considers this for a moment. He recognizes his role as magistrate is to consider the suspect's rights fairly. "Yeah, but it says he's young," he notes. "Eric doesn't sound young on the phone."

Kevin reluctantly agrees that Eric doesn't sound young—for a hacker. But he has another, more compelling argument. "OK, but how many hackers who have access to BANCS are going to be snitched on, and are going to ask specifically for Steve in the security department?" Kevin seems to have a point. He had told Eric about Steve Dougherty, one of the Pac Bell investigators who searched his condo in Menlo Park.

"All right, you win," Ron declares. "You've got probable cause."

Kevin is pleased at having won his wiretap order through a fair, judicious proceeding. He knows he had to fight for the tap just like an assistant U.S. attorney, and he knows that Ron gave it a lot more consideration than the countless federal judges who routinely rubber stamp applications for wiretaps.

A straight SAS tap is out of the question because Eric's phone service is through an old electromechanical switch and he would likely notice the click. But Kevin's got just the thing. He takes one of the clunky metal federal taps he swiped from a B box and installs it in the phone closet of a random business on Cahuenga in Hollywood. He connects the side that normally would run to the federal building to a phone line that he juices. Next, he bridge lifts the Cahuenga line to Eric's Sunset central office, where he cleverly wires it to Eric's line on a place on the frame where he'll never find it. Finally, Kevin dials the new line he's created at the Cahuenga phone closet with SAS.

There's no click on Eric's end, and if someone happened to dial the number he just created all they would get would be a disconnect recording. It's not just ingenious. It's a good example of the level of sophistication the feds might employ if they wanted to make their taps harder to detect.

Two days after putting up the tap, Kevin has listened to several of Eric's calls to Freja, when he hears him phone a friend and announce,

"You  
crafte  
Eric n  
probl  
every  
him u

Kevin  
couple  
ing lo  
Ke  
Bell's  
to talk  
"T  
begin  
Ke  
betray  
"N  
lying  
about  
"O  
"I  
"R  
Er  
"I

"You know me. I'm a live-and-let-live type of guy." The phrase sounds crafted for Kevin's ear. Although there's virtually no technological Eric might have uncovered to prove he's being tapped. But there's one problem even Kevin can't avoid. Eric, being a wiretapper himself, has every reason to assume that Kevin can't resist the temptation to put him under electronic surveillance.

---

Kevin phones Eric and suggests a face-to-face meeting. They meet a couple of blocks from Eric's old Sunset apartment, in the crowded parking lot of Ralph's Supermarket.

Kevin starts by confronting Eric with the evidence he's found in Pac Bell's security files that suggest Eric's informed on him, but Eric wants to talk about something else.

"There's something I can't tell you, something about my past," Eric begins mysteriously.

Kevin doesn't see what Eric's past can possibly have to do with his betrayal. "What, you mean that you informed on your friends?"

"No, what I mean is there is a reason I'm here in L.A., a reason underlying everything I'm doing here, and I can't tell you anything more about it."

"OK, Eric. Great. So why'd you rat on me?"

"I wouldn't snitch on you."

"Really. Then what about this tip?"

Eric laughs, a quick, short, humorless laugh.

"I'd just have you killed."

## GRAND JURY

**D**etective Bill Spradley is an old-fashioned cop fighting an old-fashioned war. He joined the LAPD in the early seventies and worked Hollywood vice, battling the tide of hookers working Sunset and the streets beyond. Work began with roll call at three-thirty in the afternoon. Dinner was something bought at McDonald's or Pioneer Chicken and eaten out of Styrofoam on the hood of a car. Spradley would start by picking up a rental car or an old junker from Bundy's Rent A Wreck, and despite his slim build, mild demeanor, and meticulous grooming, he always managed to look the part of a man on the make.

Spradley had a job that might drive some men crazy. Every night it was his duty to pick out a prostitute, invite her into his car, get her to solicit him, and then, if he was lucky, maneuver the car and his companion back to the designated arrest post before she caught on. On a good night he'd arrest several girls before his shift ended at 3 A.M. He'd get home and to sleep by about four-thirty and then rise about a quarter past seven to be ready to testify in court.

Over the years he'd had a number of close calls. Sometimes when a prostitute realized he was a cop, she would try to leap from his moving car. Other times they'd jam their high heels on the accelerator or reach for the keys. The desperate ones would lunge at Spradley and grope for

his gu  
revolv  
Un  
he'd se  
story f  
told hi  
Anoth  
said sh  
body e  
Wh  
Someo  
body k  
might,

"Please  
asks.

"La  
cop in  
Bell."

"TH  
Cro  
the sta  
before  
vides  
condo  
Franci  
sticker  
the pe

It's  
time m  
memo  
ment  
On wh  
what

his gun, a particularly valiant effort since early on he'd learned to sit on his revolver.

Until he heard the story in September of 1989, Spradley thought he'd seen it all. He gathered it in bits and pieces, never getting the whole story from any one prostitute. On street corners, between tricks, they told him what they knew. One said the Yellow Pages ad bill wasn't paid. Another said she knew how to get a free phone number. Still another said she knew how to get a phone number that would be billed to somebody else.

When Spradley pieced it all together he began to see a pattern. Someone in Hollywood could get free Yellow Pages outcall ads. Everybody knew somebody who told them it could be done, but try as he might, he couldn't get to that somebody to solve the mystery.

---

"Please state your name and your occupation," Robert Crowe calmly asks.

"Last name is Von Brauch, first name, Kurt," the bull-necked former cop introduces himself. "Occupation, security investigator for Pacific Bell."

"The telephone company?"

Crowe drives home the point. The telephone company itself is on the stand. The date is September 6, 1989, and once again Crowe stands before a secret grand jury. Under Crowe's direction Von Brauch provides an overview of the evidence taken from Poulsen's locker and condo, everything from pay phones to Pac Bell printouts on the San Francisco Soviet consulate, even a 660 communications panel with a sticker that states that it contains confidential material that will "bring the person into trouble with the federal government."

It's not as dangerous as Von Brauch claims. The 660 is simply a routine multiline central office phone, and the stickers are World War II memorabilia Kevin bought at a surplus store. But while the government is exaggerating, there's no doubt that Kevin is playing with fire. On what appears to be a page from Kevin's calendar, Von Brauch found what he believes to be a transcription of a private conversation of a Pac

Bell investigator who works in the department that wiretaps for the federal government.

"Is it correct to say that when the federal government, usually the FBI, obtains a court order for a wiretap, that Pacific Bell, pursuant to a contract with the government, actually conducts the wiretap?" Crowe asks.

"Yes, sir."

"Does Pacific Bell take certain security precautions to make sure the information is not disclosed to the public?"

"Our lab that performs that type of operation . . . [is] in a locked and alarmed facility. They have all papers and court orders maintained per government specifications in an approved safe. . . ."

"Did you discover in Kevin Poulsen's bedroom papers indicating that he had gained access to some of those federal court order wiretaps from Pacific Bell offices?"

"Yes, sir. We found three pieces of paper that . . . call the telephone number, the line equipment and cable and pair of the targeted telephone number."

"In this case, do we know what these were involved in?"

"Yes. The three wiretaps that Mr. Poulsen had intercepted and interfered with involved the tapping of the telephone of Ferdinand Marcos and associates."

But there's an even more startling fact that Von Brauch doesn't tell the grand jury. The Marcos tap was run by the foreign counterintelligence arm of the FBI.

"At some point, did Pacific Bell internal security people draw up a memorandum regarding Kevin Poulsen's access to Pacific Bell internal documents?"

"Yes, sir, they did."

"Did you have occasion to find this memorandum during your searches of the storage locker or of Poulsen's apartment?"

"Yes, sir, I did."

"Did  
tered the  
Crow  
image of  
equated

"Yes,  
Ramon..  
facility, a  
ered an il

"Did y  
regarding  
this parti

"Yes,  
with the

"Whc  
"He c  
Bell."

"Did  
"Yes,

Von l  
had been  
suggests  
storage r  
ranking  
numbers

"Yes,

Von Brau  
equipme  
"allows  
for routi  
tem." A  
ing unit  
within t

"Did you conduct an inquiry as to how Kevin Poulsen could have entered these internal Pacific Bell documents?"

Crowe's careful phrasing has a purpose. He wants to conjure up the image of old-fashioned criminal "breaking and entering," an act not yet equated with mere unauthorized computer "access."

"Yes, sir. That document involved the entry into a computer in San Ramon.... I believe the man's name was Robert Tracy at our San Ramon facility, and the contents of the memo indicated that Tracy had discovered an illegal entry."

"Did you have any conversation with Mr. Tracy or Ms. [Gerri] Lyons regarding an unusual phone call they received, an inquiry concerning this particular memo?"

"Yes, sir... there was an attempt to obtain that particular memo, with the person who was calling claiming to be someone else."

"Who did that person claim to be?"

"He claimed to be a high-ranking management official at Pacific Bell."

"Did they also give the correct callback number?"

"Yes, sir, they did."

Von Brauch first explains how he discovered the executive's phone had been surreptitiously call-forwarded to a pay phone, and then Crowe suggests a likely culprit. "Did you find in Poulsen's apartment, or in the storage room, Pacific Bell directories indicating the names of the top-ranking Pacific Bell officers, security personnel, and their telephone numbers?"

"Yes, sir."

Von Brauch mistakes some of Kevin's junk for wiretapping and military equipment. The antique three-hundred-pound TSPS console suddenly "allows an operator to break into calls..." A sixteen-button phone used for routine testing is represented as a "military communications system." A mechanized lube testing trunk test set and a direct access testing unit, or DATU, enables the hacker to tap "any telephone literally within the country."

GRAND JURY

Unfamiliar with Poulsen's electronic world, the grand jury needs a simple, physical sense of the hacker's powers, and Von Brauch's colorful descriptions seem to do the trick. "Agent Von Brauch, you have talked about a room and called it the switching room. What does the name switch room come from?"

"Switch room' is the term given to telephone switching rooms because that is basically what they are. They are in a room and they contain a telephone switch."

"Why did you refer to the room depicted in the photo as the switch room?"

"The sign 'switch room' here that you see in the left margin of this photograph was attached over the door of the third bedroom of the apartment at 1055 Pine Street in Menlo Park."

"So, in other words, Poulsen and Lottor... had placed a sign up there saying 'the switch room'?"

---

Crowe impresses upon the grand jury that the most relevant statute for their deliberation will be Section 1029 of Title 18 of the United States Code, Fraud and Related Activity in Connection with Access Devices. "Access" is the key word, and Crowe asserts that access has been obtained.

"Did your investigation come up with evidence whether Poulsen, Lottor, and Gilligan had access to various government equipment?" Crowe asks Von Brauch.

"Yes, sir."

"Let me show you this document.... Describe it," Crowe requests.

"That is a piece of electronic mail transmission we obtained from one of the data tapes that was recovered from Kevin Poulsen... mailed from Robert Gilligan...."

Von Brauch continues, stating that the mail is evidence Gilligan accessed a military network called Masnet. The printout of the network's opening screen, Von Brauch asserts, proves he broke the law. "Underneath that Masnet label is a warning that states, and I will quote it: 'Un-

authorized  
Title 18, U

"It then

"Access

"Those

comment

The ev

governm

valuable a

would be c

"Durin

from Kevi

ary record

"Yes, si

"What

"Are w

"Yes."

"I foun

ercise of t

craft, air t

gets on the

are curren

The all

hacked ac

that migh

San Franc

"Did th

level?" Cr

"Yes, s

"Did I

have acce

"None

Von Brau

But V

gan had g

authorized access to the use of this computer system is in violation of Title 18, U.S. Code, Section 1030. Violation will be prosecuted.

"It then goes on to list a menu of ways to enter the system."

"Access codes?" Crowe leads his witness.

"Those are access codes," agrees Von Brauch, adding, "There is also a comment from Mr. Gilligan to Mr. Poulsen that says, 'Check this out!'"

The evidence appears solid. Robert Gilligan had allegedly "accessed" a government computer and Poulsen allegedly had in his possession the valuable access codes. The system banner itself warned that trespassers would be charged with a felony.

"During the course of the investigation did you obtain information from Kevin Poulsen as to whether he had accessed any classified military records?" questions Crowe.

"Yes, sir, I did."

"What did you pull off the computer that indicated that?"

"Are we at liberty to discuss that?"

"Yes."

"I found a detailed air attack task order that involved a military exercise of the Eighty-second Airborne Division, which involved all aircraft, air transporters plus fighter intercept and attack orders. The targets on the fighter interception and attack orders are current targets and are currently classified."

The allegations are all beginning to tie together. Kevin Poulsen has hacked access codes to military computers and obtained something that might be of real value to the Soviet consulate on Green Street in San Francisco.

"Did this particular document indicate it was classified at the secret level?" Crowe continues.

"Yes, sir, every page listed that classification."

"Did Poulsen, Lottor, and Gilligan have appropriate clearance to have access to those documents?"

"None of them have ever obtained any level of security clearance," Von Brauch states.

But Von Brauch is at least partly mistaken. Both Poulsen and Gilligan had government security clearances.



The grand jurors have a few questions for Von Brauch about the motivations of the hackers' eavesdropping. "Did you find a specific reason why they were doing it? Was it just a prank?"

"The one that was done on the college we believe was an experimental type of tap," Von Brauch begins. "... The taps of the family ... down in the North Hollywood area, the one young lady was an ex-girlfriend of Kevin's. ... The third one, which I don't believe we included here, was Molly Ringwald. Apparently he had a fixation with a certain number of stars, Janis Quey, Molly Ringwald, and I believe there was a third one."

"The equipment that they had," probes the persistent juror, "is there evidence of their using it for their own benefit ... were [they] selling any kind of service with the equipment that they had?"

It's a good question, but neither Von Brauch nor any other federal witness called before the grand jury has an answer. And some basic questions need answering. Ignorant of Poulsen's mastery of SAS, the government can only guess at how he's wiretapping. And there are other mysteries. Why had this young man stuffed his apartment with swiped and scavenged telephone equipment? Why had he walked straight into the phone company's downtown San Francisco headquarters to have the run of its security offices? How did he know about the federal Marcos spy taps and possess phone records of the Soviet consulate and what appeared to be classified military documents? And, most of all, what did he plan to do with all of his secrets and access?

squints at t  
A.M., and he  
to penetrat  
he set the a  
continues  
convertible

Ron sw.  
on it. How  
He crushes  
swearing, .  
Maserati a

For the  
everything  
from sever  
KLSX to p  
day of the  
teners that  
magic opp